NORTHERN ARIZONA UNIVERSITY

INF638/9: topics in Cybersecurity

- INF638 : *Elements of Cryptography*
- INF639: *Nanotechnologies for cybersecurity*

Grading INF639 Spring 2019

Assignment		Weight %
Attendance (no miss, no late, no early departure: 100%) miss 1 week: 75% (10% per hour) miss 2 weeks: 50% miss 3 weeks: 25% miss 4 weeks: 0% **Important:** you are not tested in this class, however if you miss a class you have the opportunity to be tested on this class during office hours to gain back the lost points		15%
In class assignments	Project presented in class: 25% each Volunteer to participate to in class event : 10% each	15%
Homework assignments	85%: 100% 75%: 90% 2/3: 80% 0-50%: 0-50%	15%
Research project #1:	Demonstrate understanding of the basic concepts	15%
Research project #2:	Demonstrate understanding of the advanced concepts	15%
Research project #3:	Demonstrate ability to implement and generalize	15%
Final report:	Ability to offer synthetic view	10%

NORTHERN ARIZONA UNIVERSITY

INF 639: Nanoelectronics for cybersecurity

1.	From Micro to Nano-electronics	
2.	Introduction to cryptography	CS/EE
3.	Public Key Infrastructure	CS/EE
4.	Smartcards	
5.	Attacks on smartcards	
6.	MOS transistor & logic circuits	EE
7.	Biometry	
8.	Physical Unclonable Functions (PUF)	CS/EE
9.	Access control and authentication	CS/EE
10.	Flash Memory devices & security	EE
11.	Resistive RAM & security	EE
12.	Public key cryptography with PUFs	CS
13.	Sensor devices and security	EE
14.	Ternary cryptography	

NORTHERN ARIZONA UNIVERSITY

INF639: Nanoelectronics for Cybersecurity

Section 1: From Micro to Nano-electronics

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu

NORTHERN ARIZONA UNIVERSITY

1 From Micro to Nano-electronics

- 1- Motivation for INF633/EE599
- 2- From 1µm to 45nm – the Moore law
  - The MOS transistor - limitations
  - Path to 45nm
- 3- From 45nm to 10nm – 3D transistors
- 4- From 10nm to 1nm – Nanotubes
- 5- 3D integration – Stacking silicon together

A Connected Environment

NORTHERN ARIZONA UNIVERSITY

SMART CITY

Smart medicine

Smart retail

Smart home

Smart agriculture

Connected cars

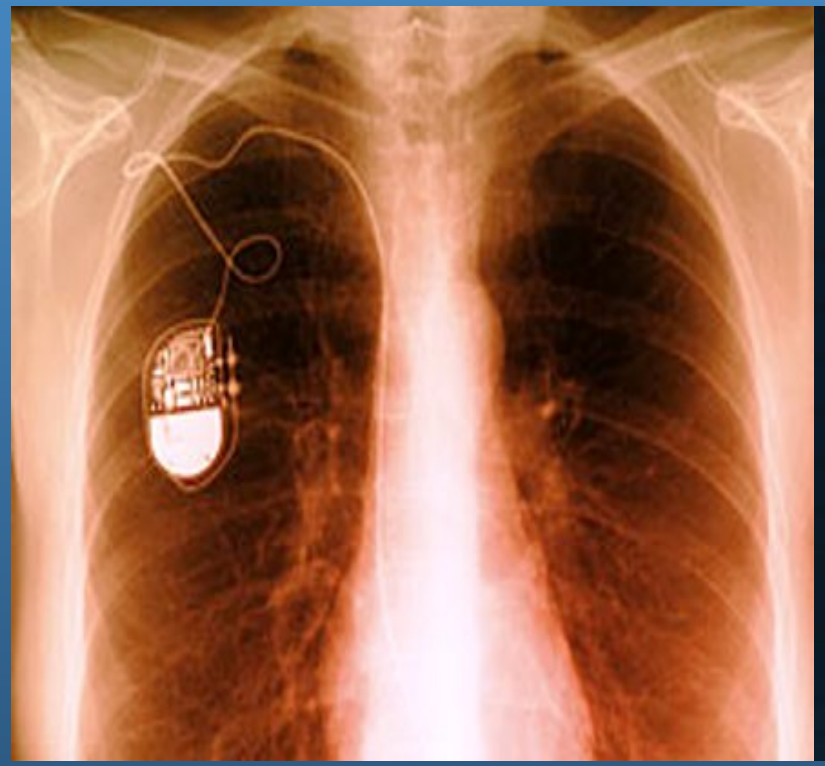
Smart industry

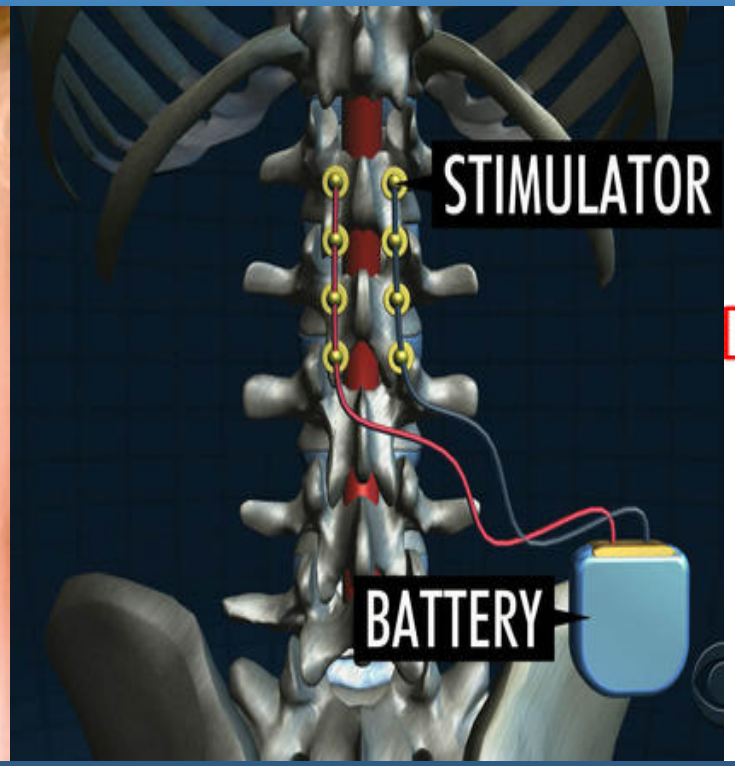
Smart energy

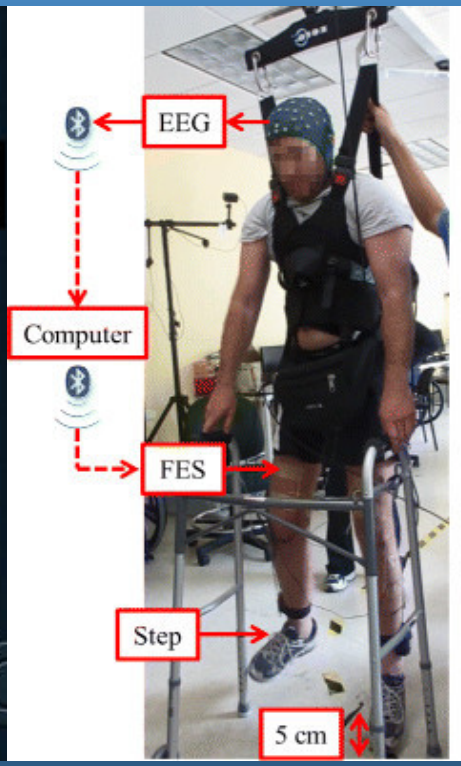
Internet of Things

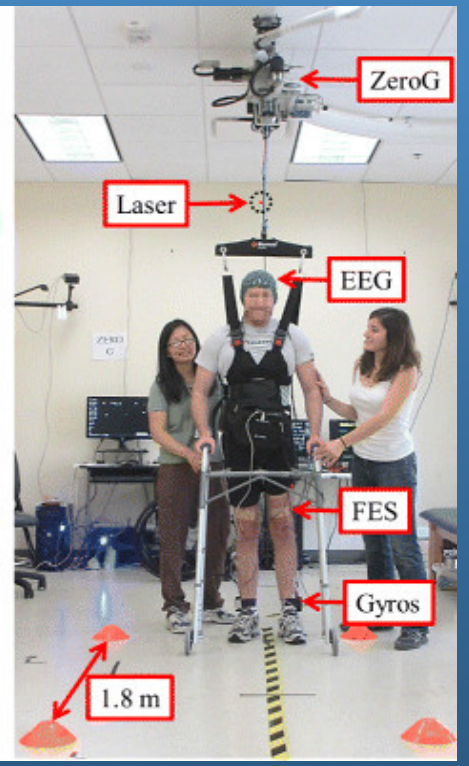
Example: People connectivity & biomedical advances

Electric stimulators: Muscle activation, heart, neurology,…
Biochemistry: Blood composition, bacteria measurement,.
Vital signs: Temperature, blood pressure, heart rate,…
Optical sensing: Collision avoidance, recognition algorithms,.
Mechanical: Pressure sensor, acceleration, rotation,…










NORTHERN ARIZONA UNIVERSITY
Why is it so difficult to block cyberattacks?
Learning from the past don't always prevent future breaches
Firewalls, antivirus, artificial intelligence recognize previous attacks

A- Learning from the past will not prevent future breaches

Malware, worms, and virus inserted by malicious entities

As much as one million new malware born everyday

"Worms" can be dormant years before activation

Breaches in access control

Due to PW guessing, identity theft, insider attack.

Eavesdropping

by institutions over the years, over open network

Man-in-the-middle attacks

Malicious agents pretend to be legitimate actors

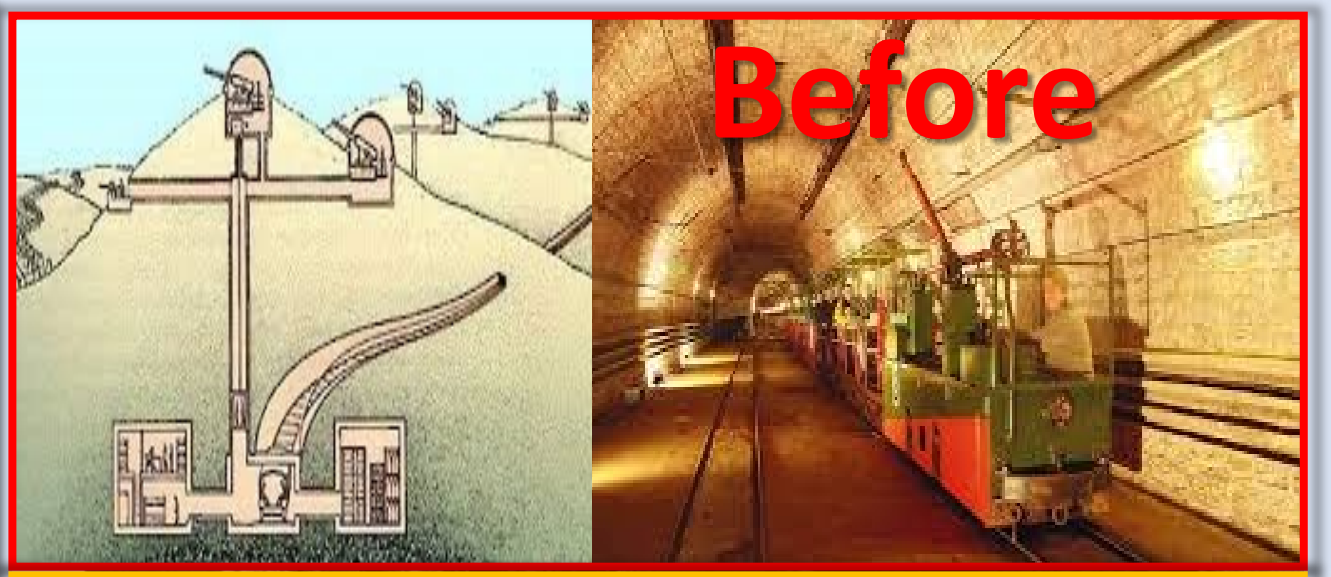
Protocol-based attacks

The attacker has access to the security protocols

Interaction with people and social engineering

Example of the Maginot line

Learning from the past will not prevent future breaches



Before

After

Bundesarchiv, Bild 121-0486

Example of “Maginot line” practices:

1. Use over-complicated PW for different applications:
   can we remember these PW?
2. Change your PW frequently :
   what are the risks associated?
3. Download the latest SW revision (Window/Mac, Office, Adobe,..):
   what about illegitimate requests?

Example of rarely enforced practices:

1. Encrypt sensitive messages
   for example adobe pro with AES encryption
2. Use of multi-factor authentication
   avoid the reliance on password change
3. Use of chip cards with public keys
   avoid key distribution & use RSA, ECC, SHA, AES

B- IoTs security is often not adequate

Breaches in access control:

- Billions of exposed nodes and sensors
- IoTs can have inadequate power for cryptography
- loss of the IoT to malicious parties
- Side channel attacks

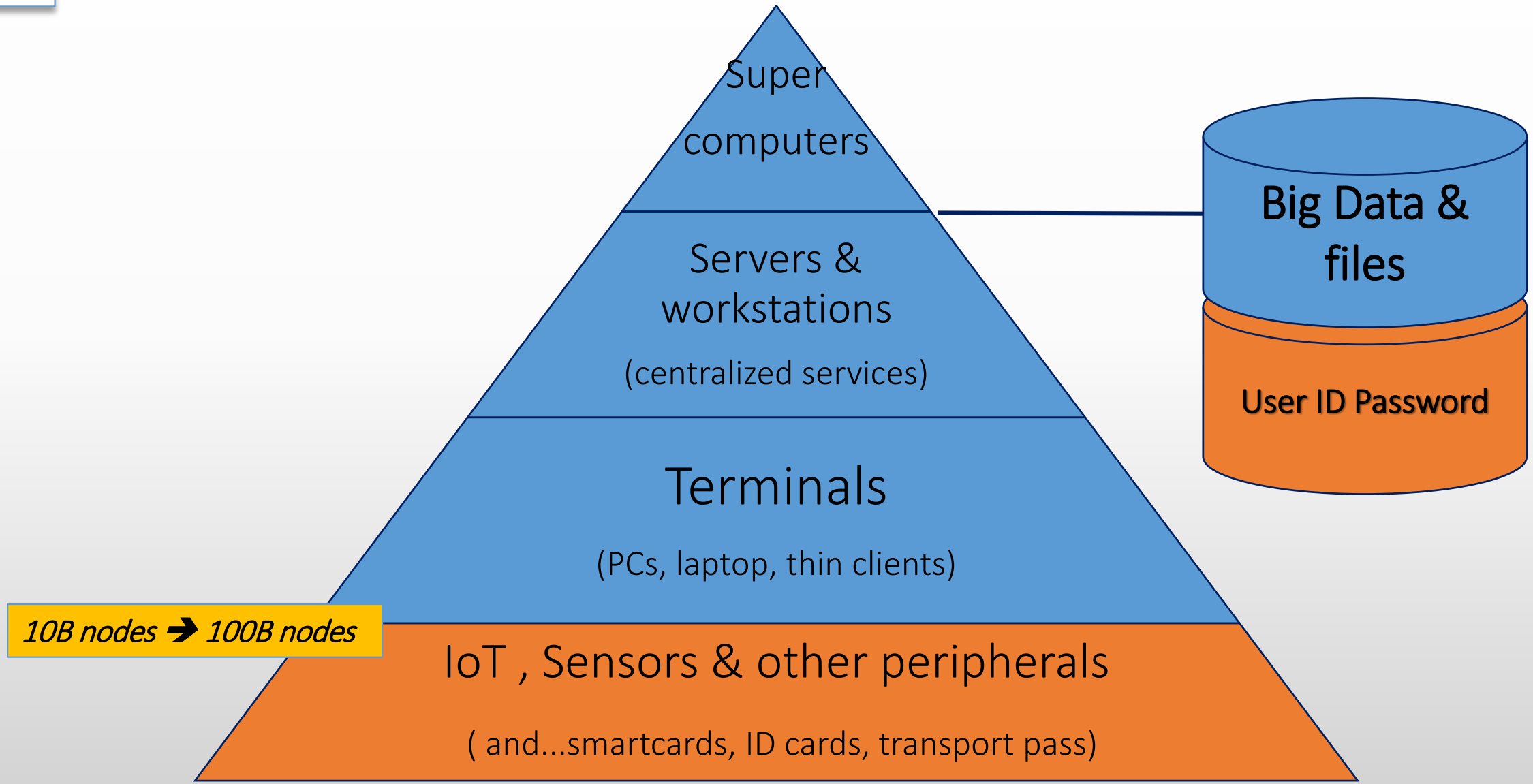
Man-in-the-middle attacks:

- Lack of uniform security architecture of the IoTs
- Exposure of the weakest link

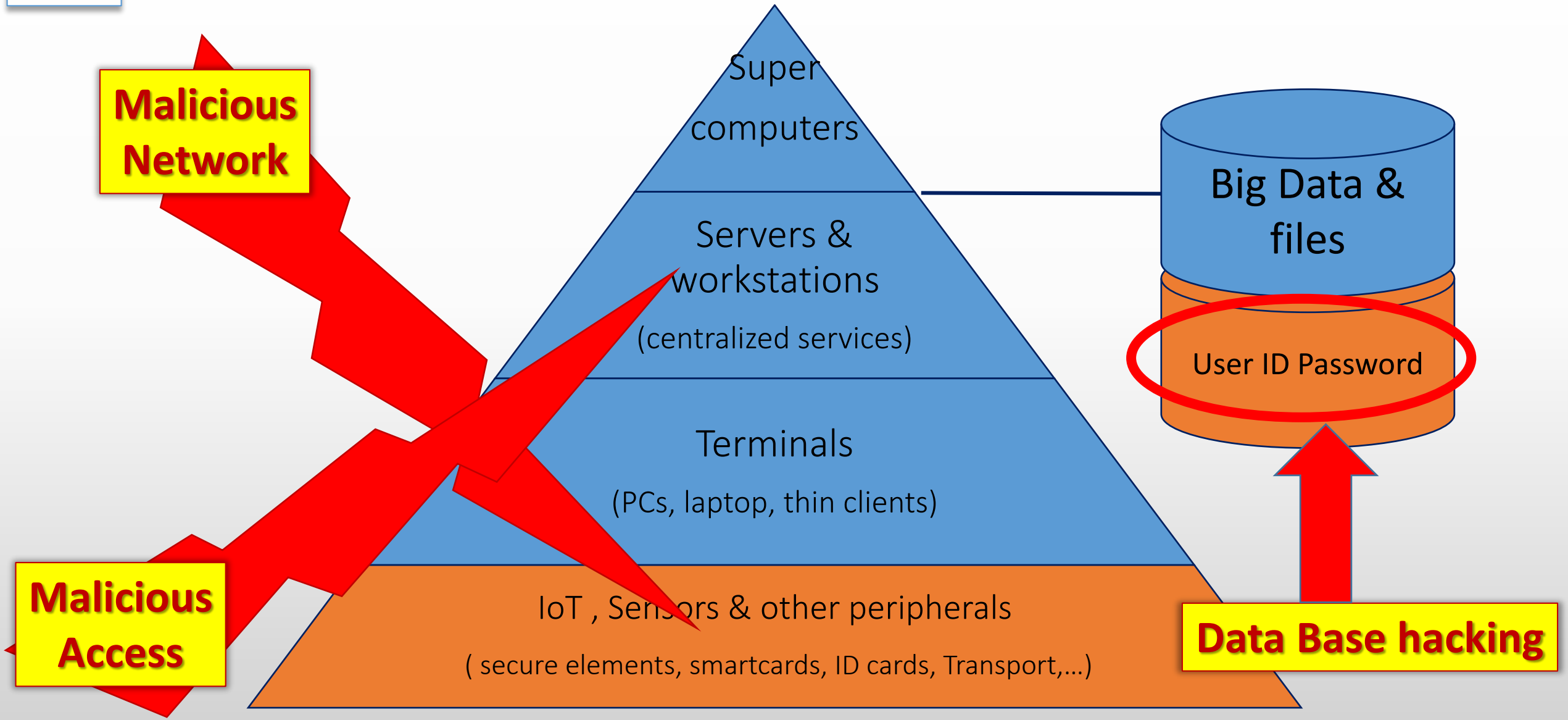
Distributed denial-of-service (DDoS):

- Attacks overwhelm the communication server-client

Cyber Physical Systems CPS



Cyber-attacks of CPS



C- Quantum computers will challenge cryptography

- QC will break modern cryptography in seconds
- QC are expected to be powerful enough within 3-10 years

The international race to develop QC to break RSA and ECC has started

Vision: nanomaterials to protect strategic assets

Two-way Authentication
Secure access control
Secure cryptography

Strategic asset

Crypto-protection With Nanomaterials

Traditional environment HW/SW

Server

Crypto-processing With Nanomaterials

Traditional environment HW/SW

Why nanomaterials?

Micro-electronic components are now using nanomaterials

1µm (10^{-6}m) geometry in the early 90's ➔ 10nm now

➔ 1nm (10^{-9}m) expected in 2027

This represents less than 10 atomic layers

Each component is subject to manufacturing variations:

Almost unique

Unclonable

We can extract electronic "fingerprints" from the nanostructures

These "fingerprints" are called Physical Unclonable Functions (PUF)

We can develop a new class of cryptography based on PUFs

Several orders of magnitude more protective than traditional cryptography

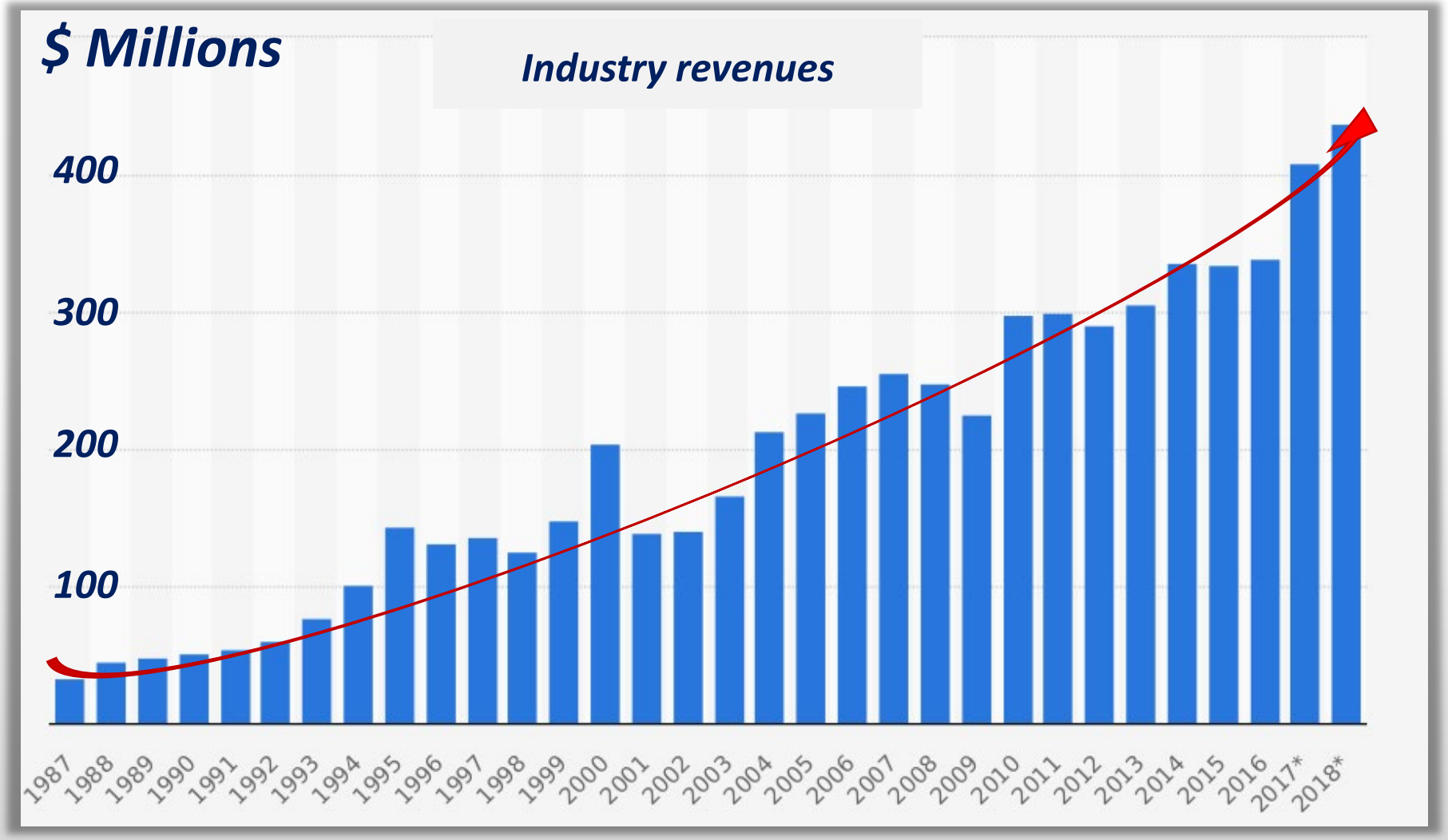
Opportunity to be quantum computer resistant

NORTHERN ARIZONA UNIVERSITY

1 From Micro to Nano-electronics

- 1- Motivation for INF633/EE599
- 2- From 1µm to 45nm – the Moore law
  - The MOS transistor - limitations
  - Path to 45nm
- 3- From 45nm to 10nm – 3D transistors
- 4- From 10nm to 1nm – Nanotubes
- 5- 3D integration – Stacking silicon together

Expansion of the Semiconductor industry



WSTS forecasts:

2016: $339B

2017: $408B

2018: $437B

In Arizona:

Intel Corporation

On Semiconductor

Freescale-NXP

Microchip

ASML-America

Soitec-America

FlipChip technologies

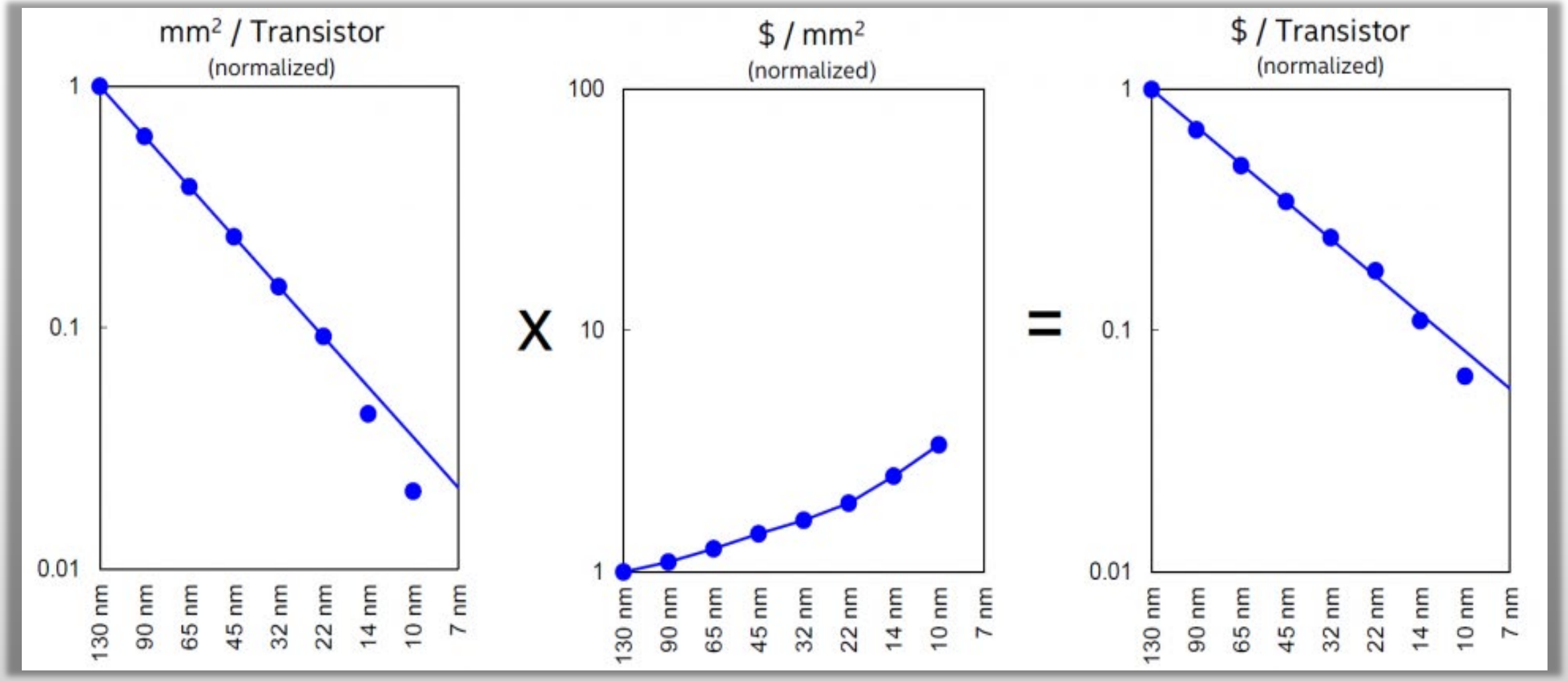
AVNET

AMKOR

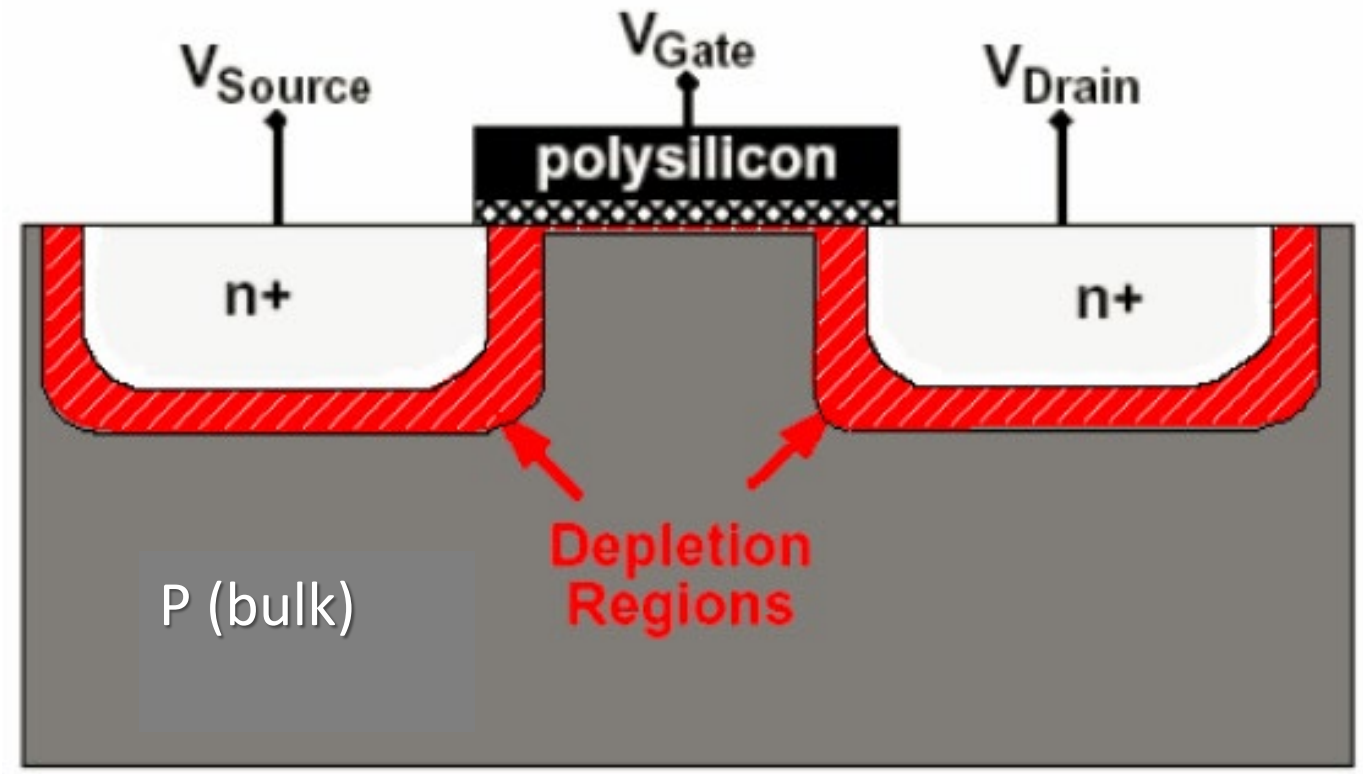
Medtronic

Maxim

Moore's law: Double transistor density every 2 years
(An update from Intel)

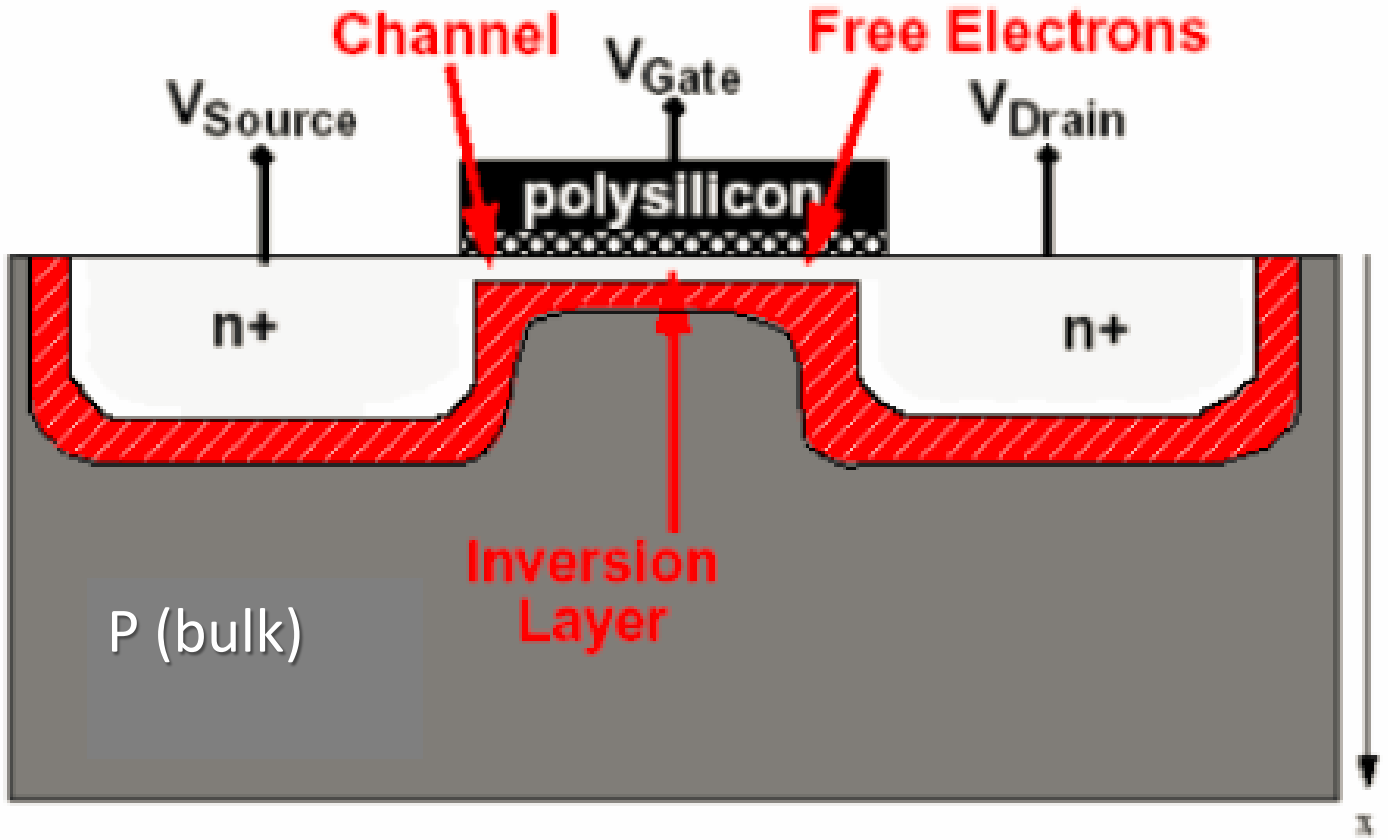


NMOS transistor: Sub-threshold operation



$V_G < V_t$ → Low I_{DS} current

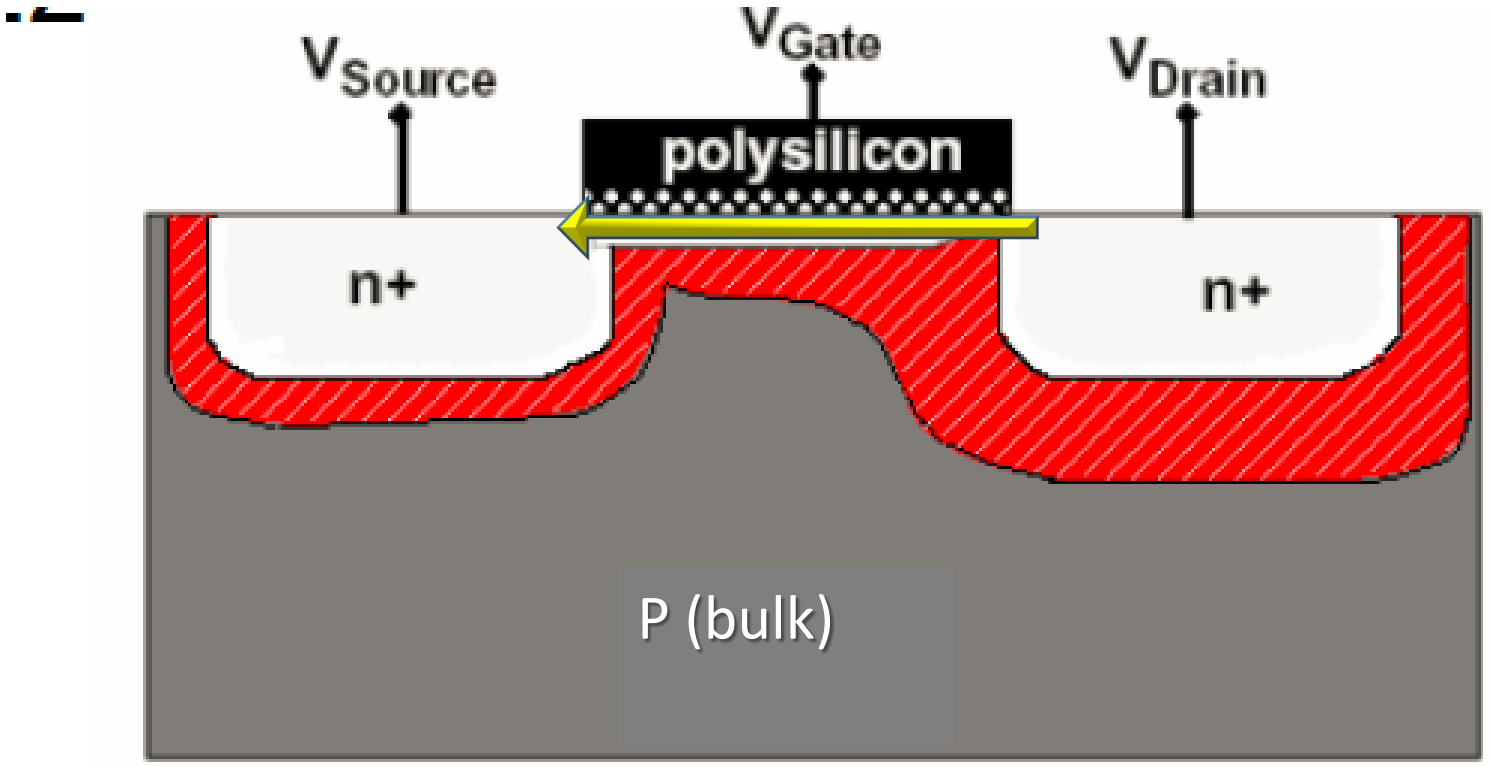
NMOS transistor: Low V_{DS} operation



V_S=0V V_G=1V V_D=0V

VDS=0 $V_G > V_t$ → **No I_{DS} current**

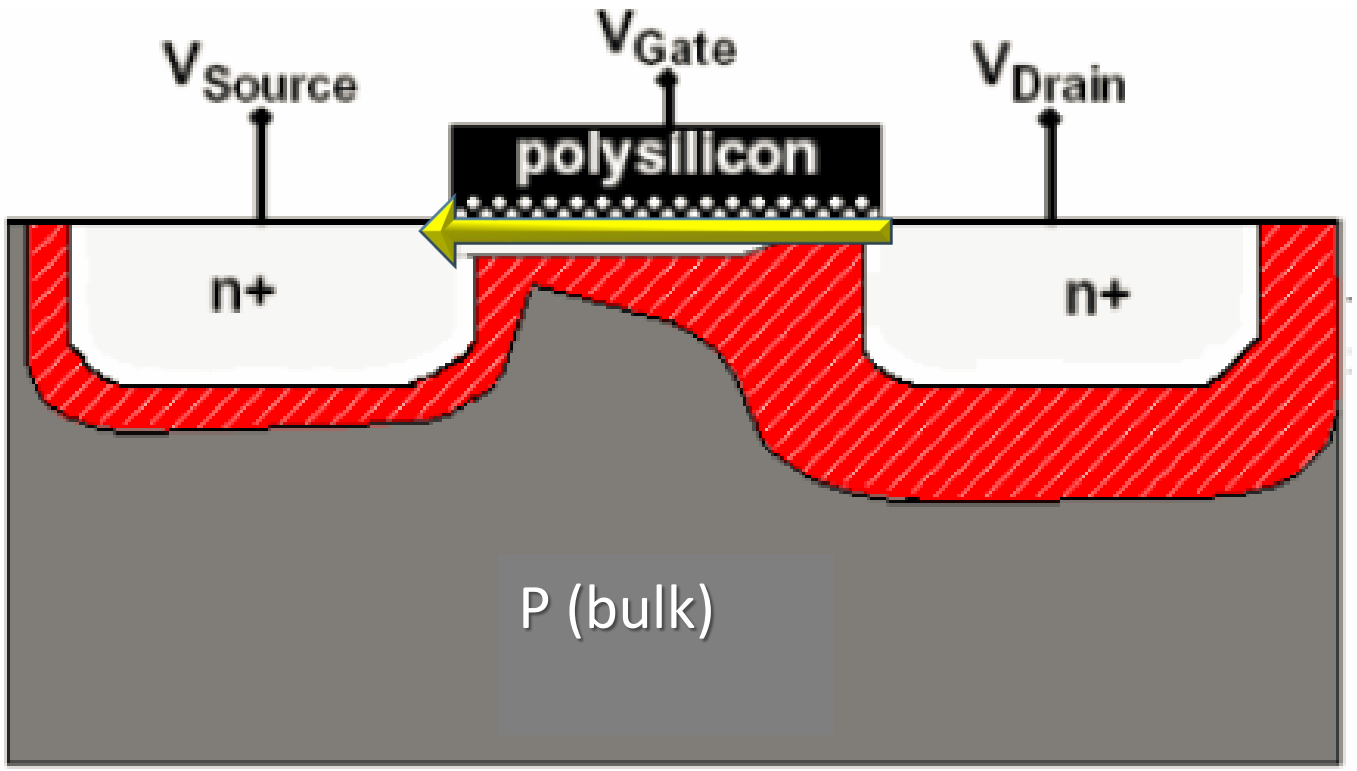
NMOS transistor: Conducting mode



V_S=0V V_G=1V V_D=0.25V

VDS>0 $V_G > V_t$ → **I_{DS} current**

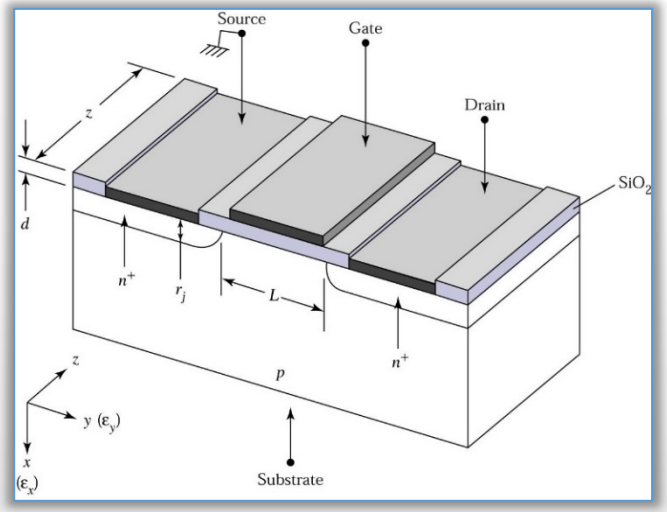
NMOS transistor: saturation mode

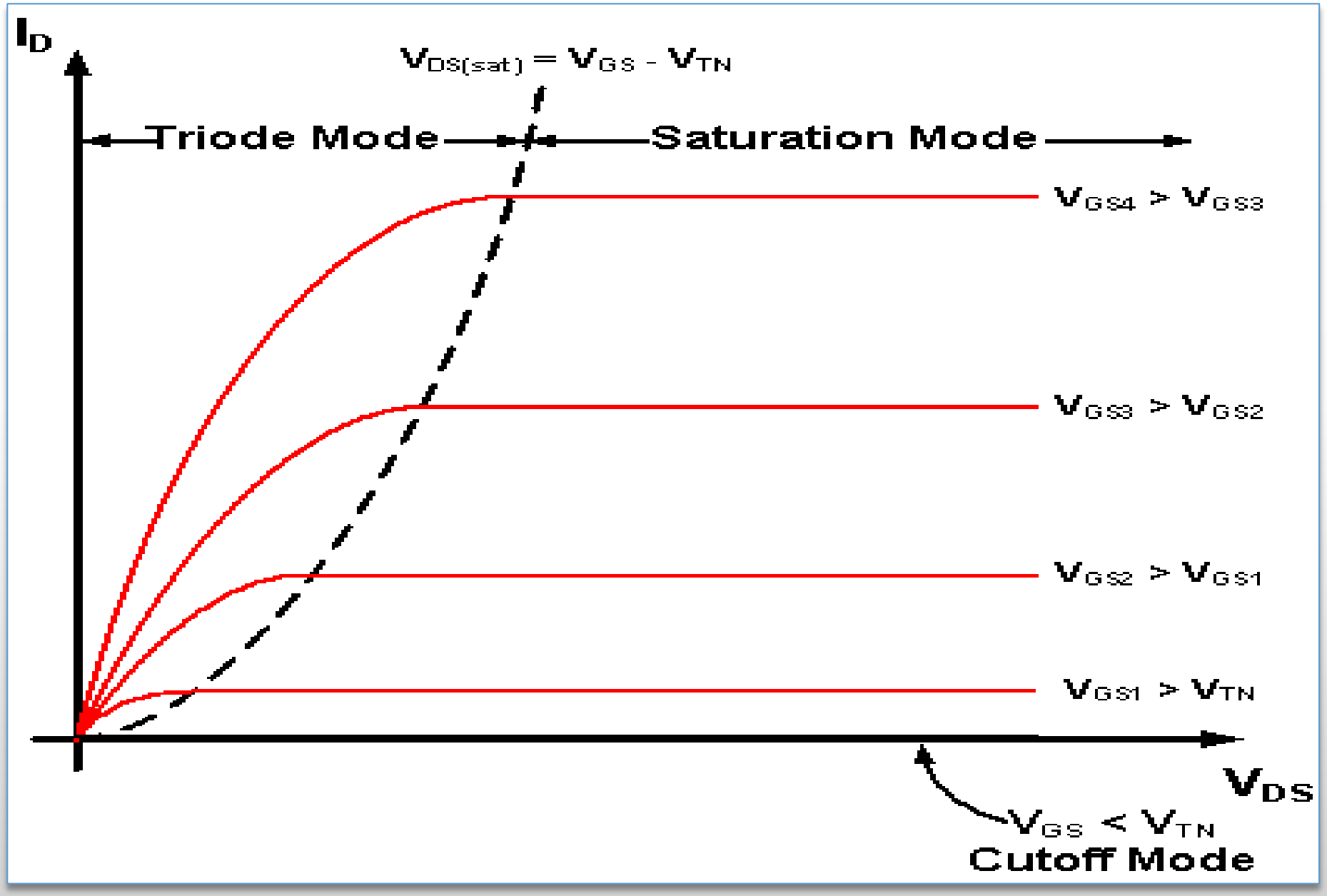


V_S=0V V_G=1V V_D=0.35V

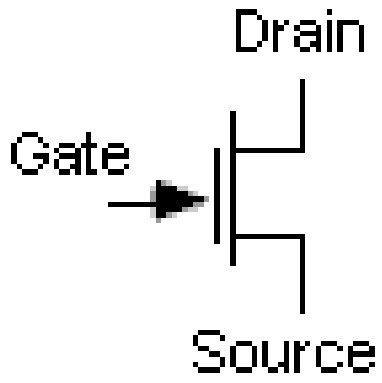
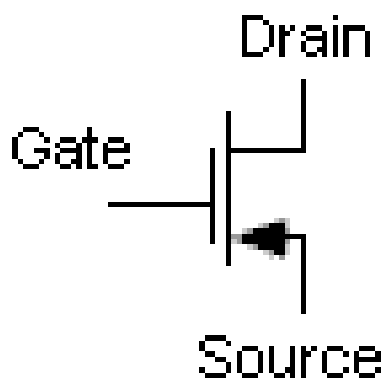
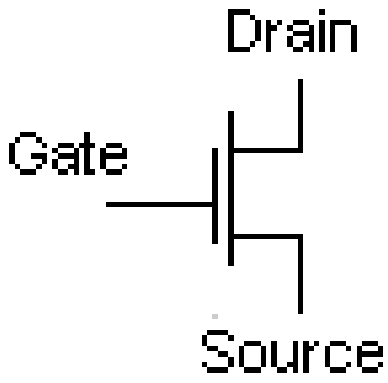
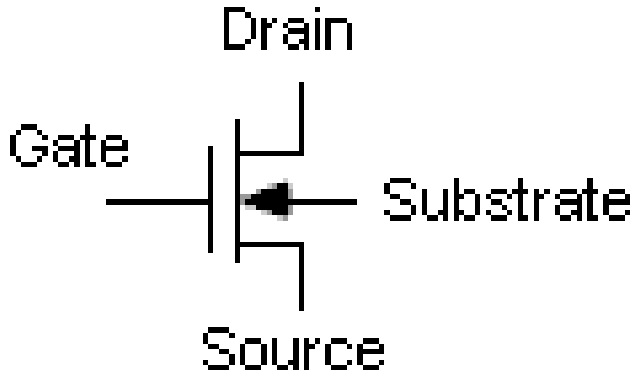
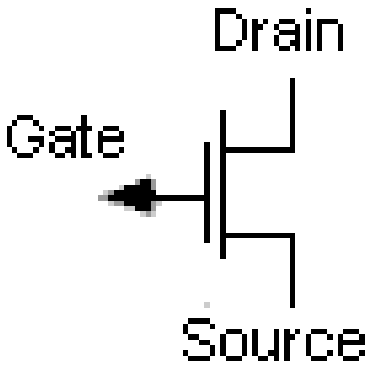
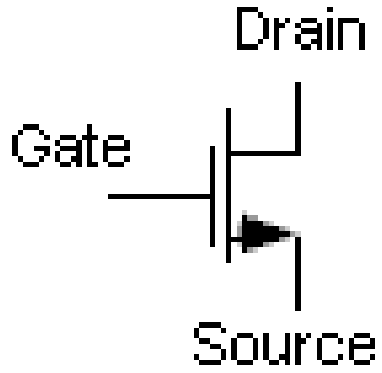
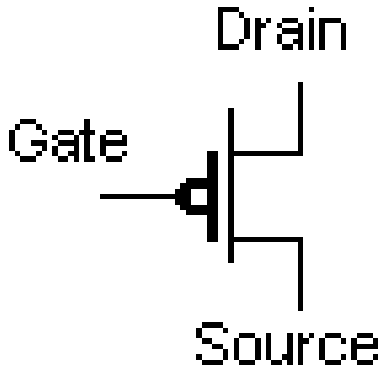
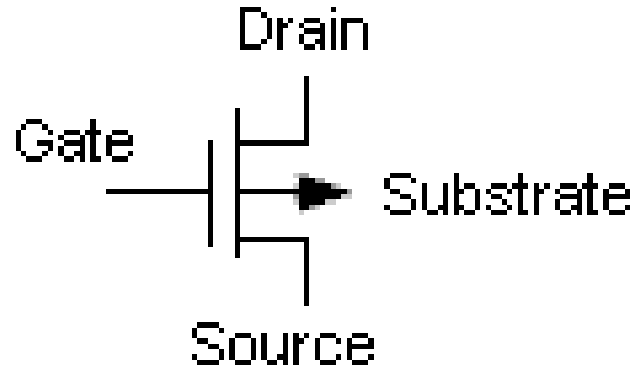
VDS>>>0 $V_G > V_t$ → **I_{DS} Saturation**

NMOS transistor trans-conductance



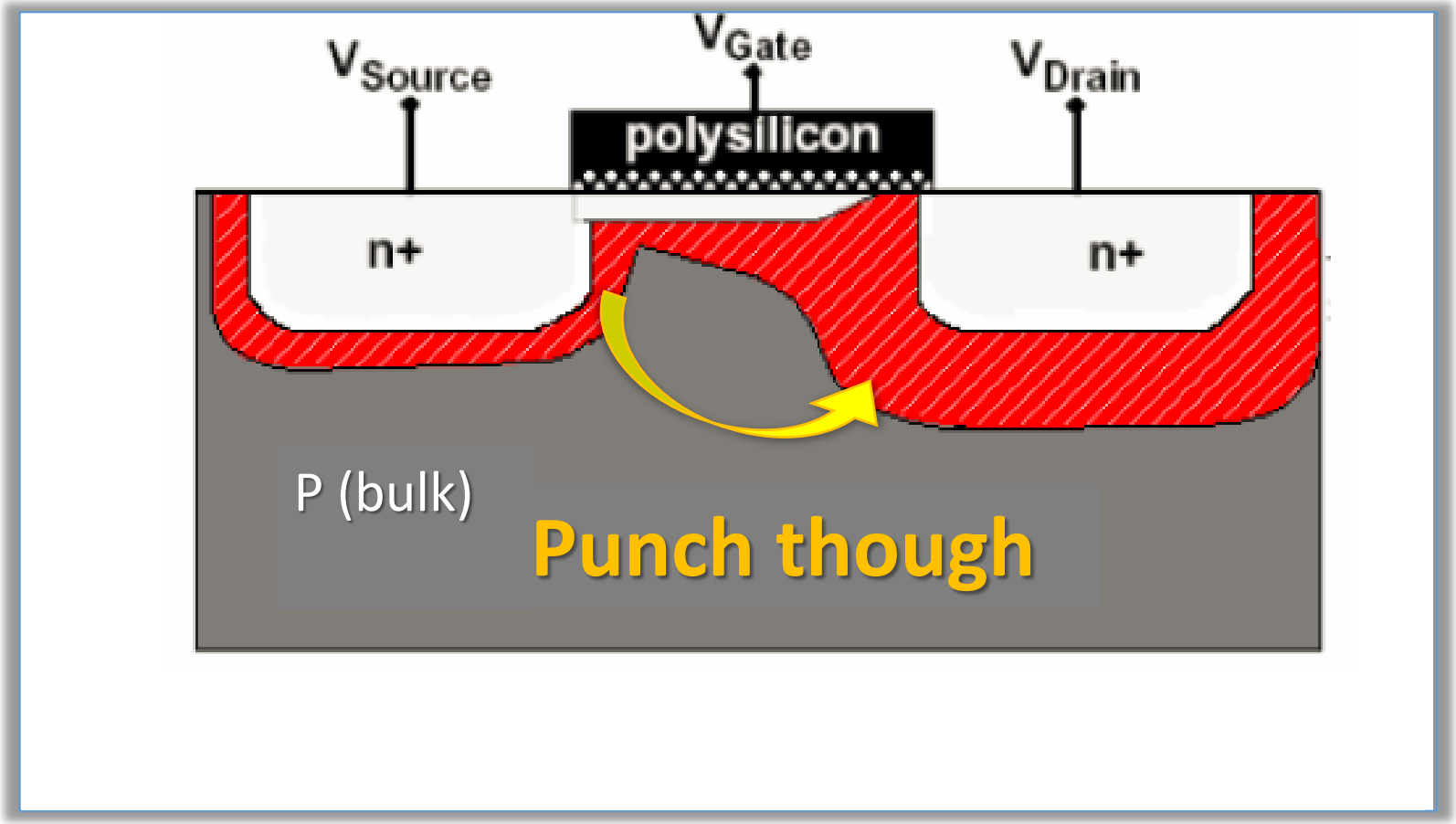


NMOS and PMOS transistor symbols

NMOS				
PMOS				

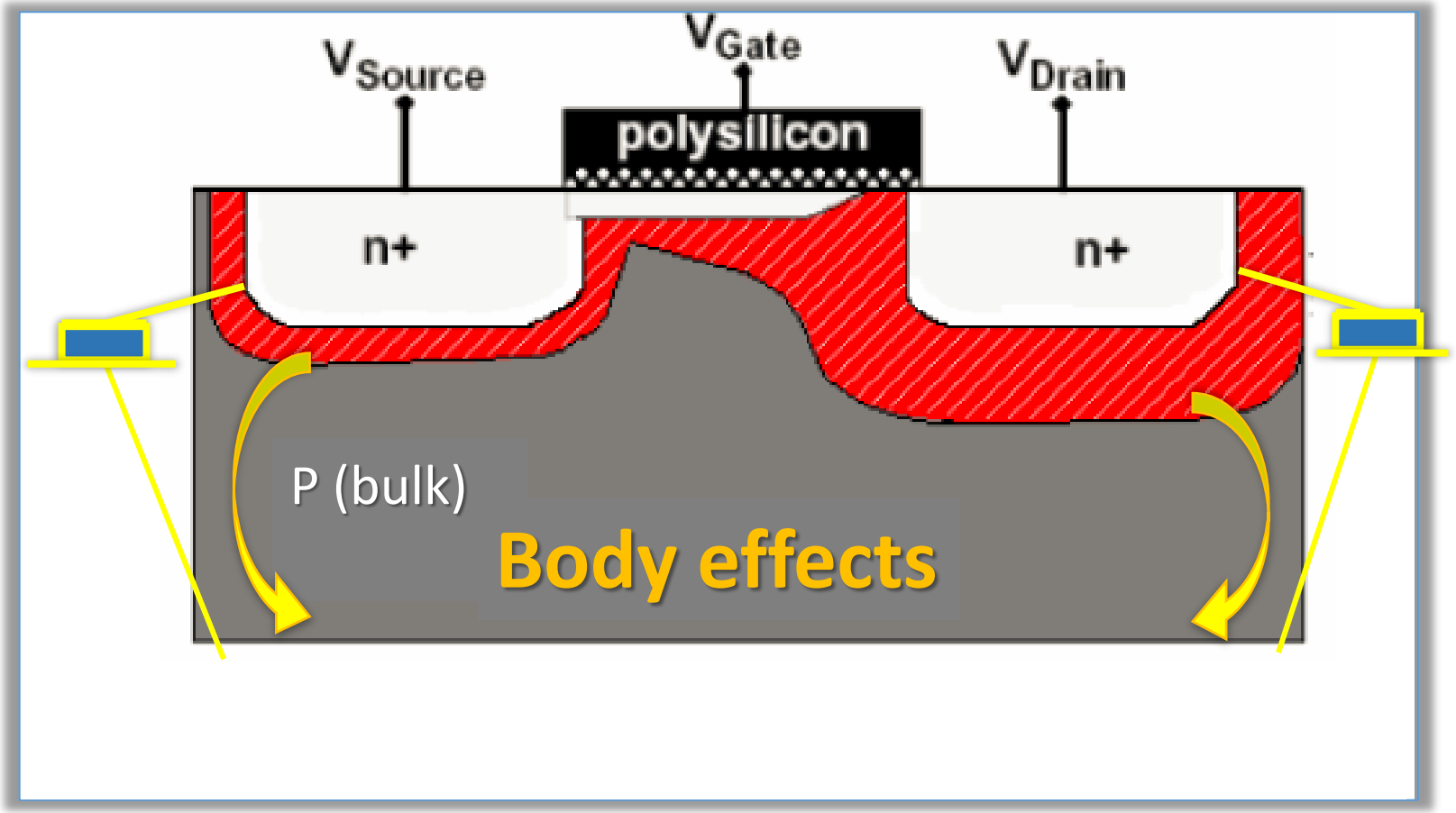
Effects due to size reduction: Short Channel effect

- Punch through (parasitic BJT)
- Narrow width effects



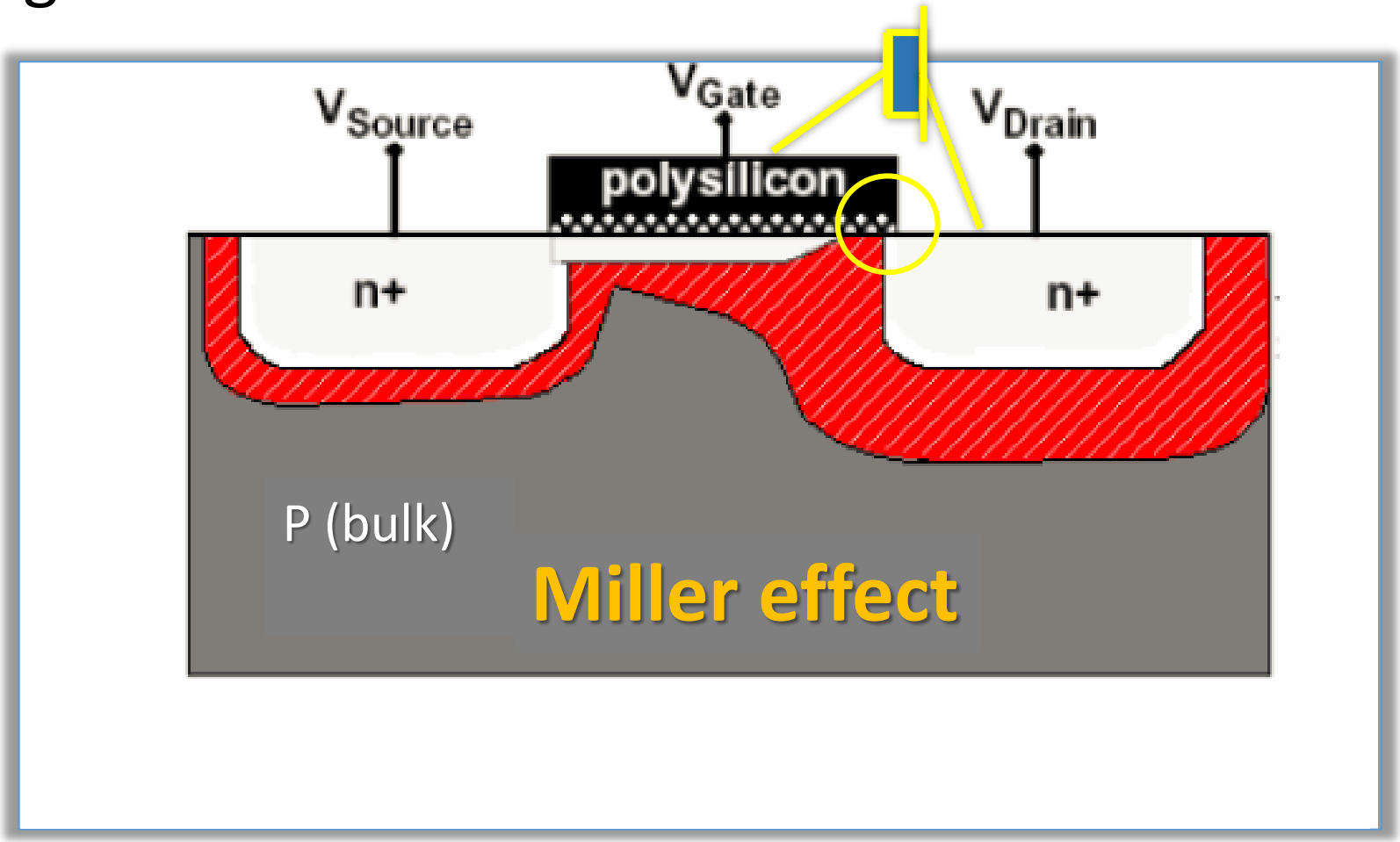
Effects due to size reduction: Body effect

- Leakages
- Parasitic capacitances



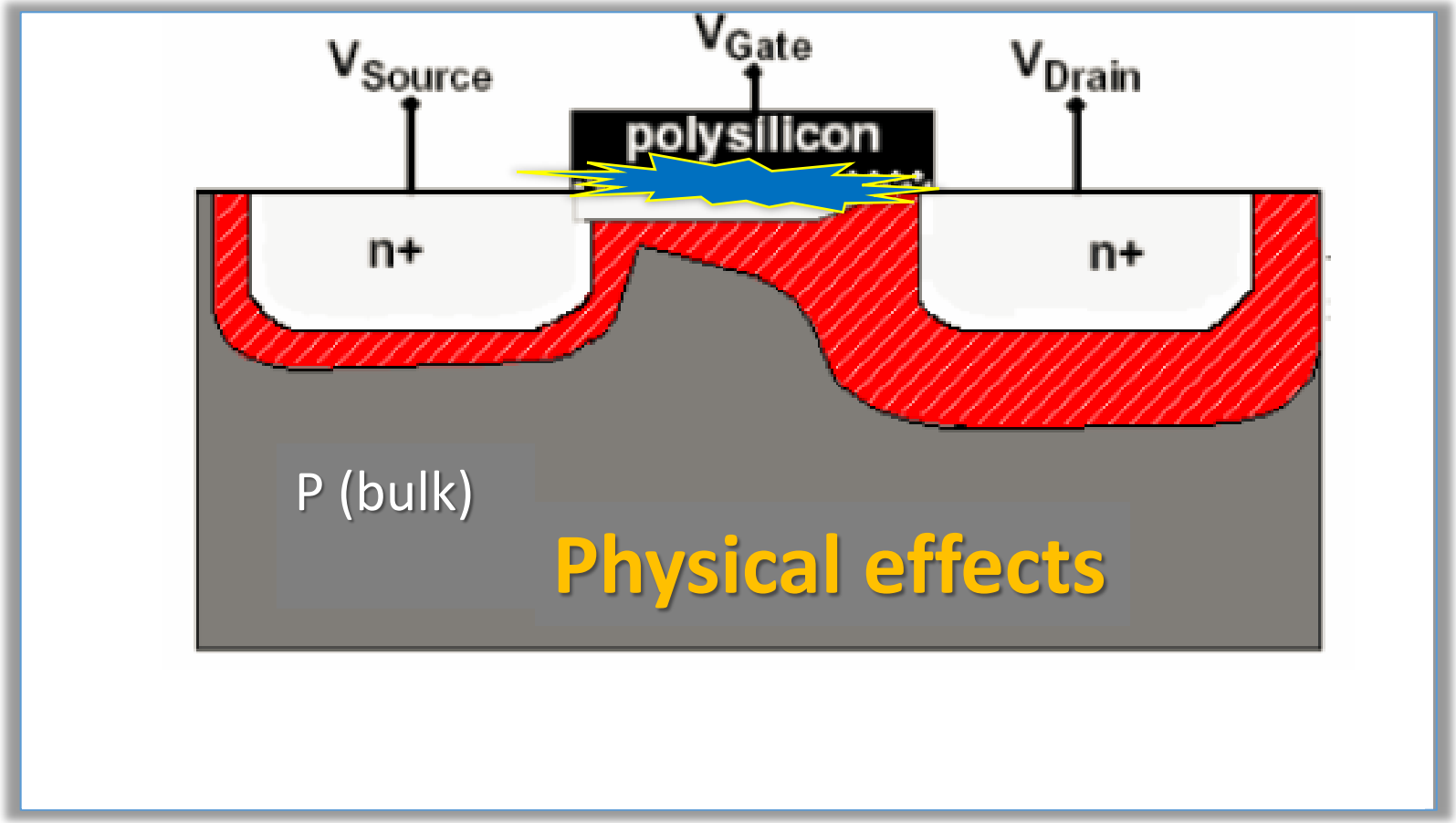
Effects due to size reduction: gate/drain coupling effect

- Miller effect ➔ Gate to drain capacitances
- Vt too high ➔ Gate thickness cannot be reduced



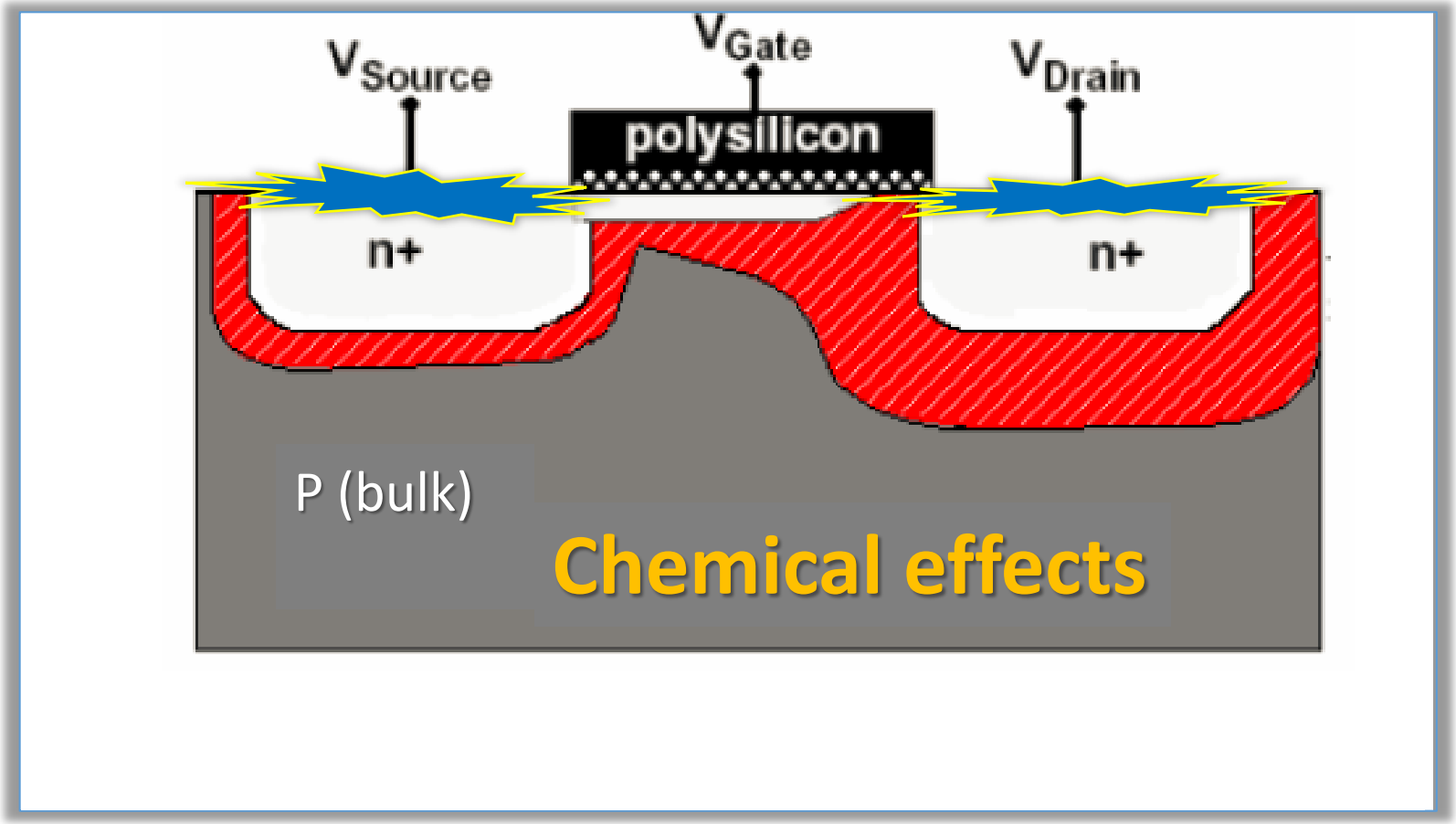
Effects due to size reduction: Physical effects

- Hot carrier effect → electron trapping in the gate → Vt drifts
- Effect of Si/SiO2 surface scattering → Mobility reduction



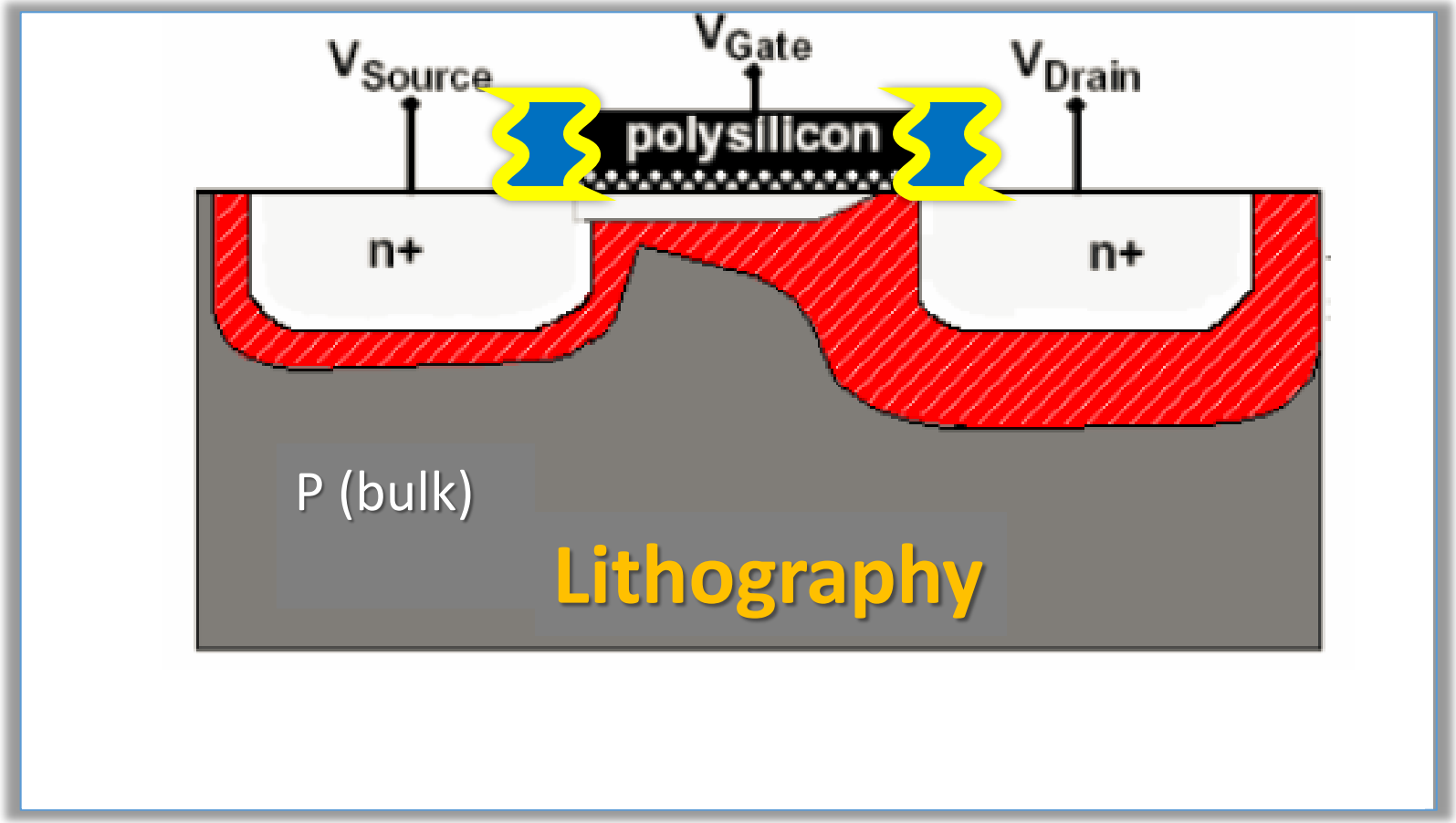
Effects due to size reduction: Chemical effects

- Electro-migration of metallic elements from the contacts and the gate to the channel



Effects due to size reduction: Optical interferences

- Scattering of the light during lithographic steps
- Mask fabrication is increasingly difficult



Effects due to size reduction

- Short Channel effects
  - Punch through (parasitic BJT)
  - Narrow width effects
- Body effects
  - Leakages
  - Parasitic capacitances
- Gate coupling effects
  - Miller effect ➔ Gate to drain capacitances
  - Vt too high ➔ Gate thickness cannot be reduced
- Physical effects
  - Hot carrier effect ➔ electron trapping in the gate ➔ Vt drifts
  - Effect of Si/SiO2 surface scattering ➔ Mobility reduction
- Chemical degradation
  - Electro-migration of metallic elements from the contacts and the gate to the channel
- Optical interferences
  - Scattering of the light during lithographic steps
  - Mask fabrication is increasingly difficult

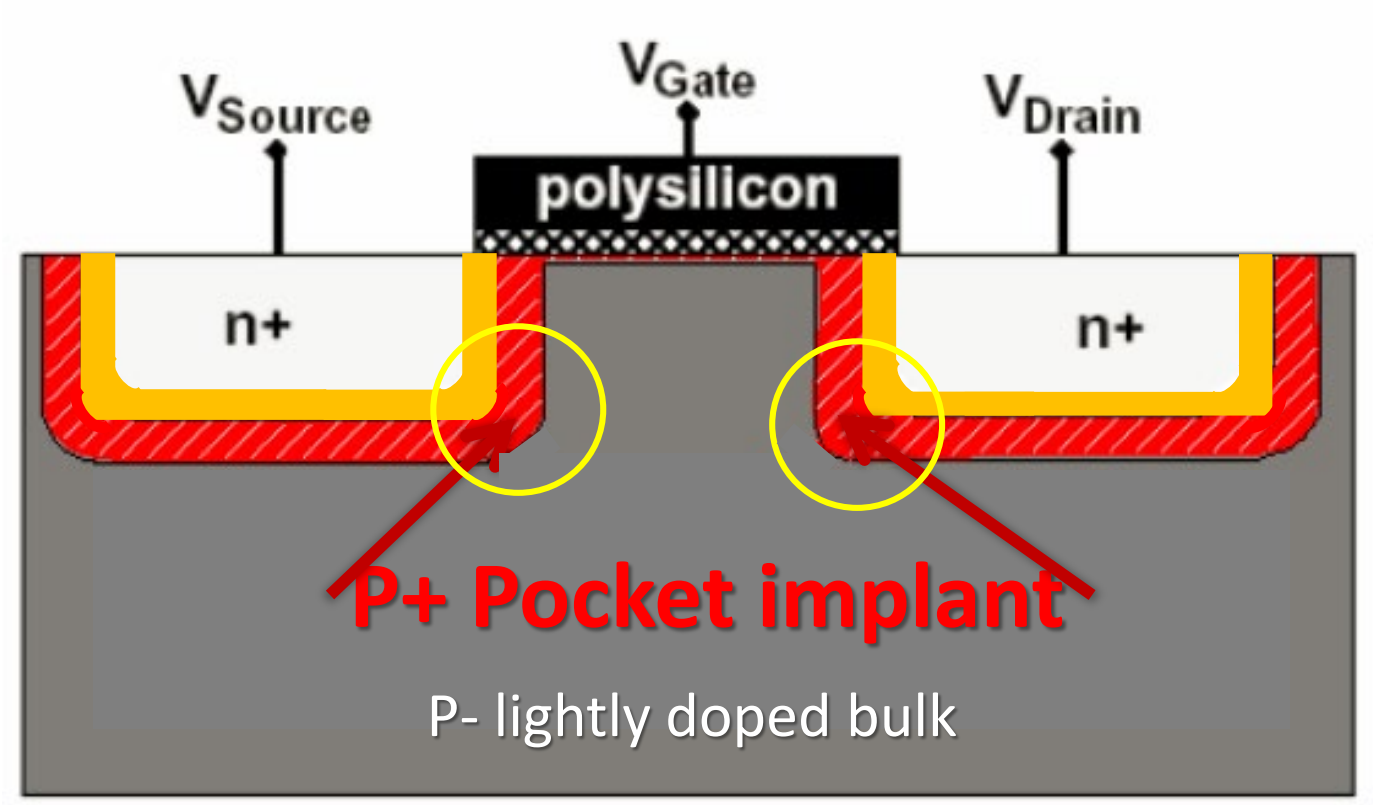
NORTHERN ARIZONA UNIVERSITY

1 From Micro to Nano-electronics

- 1- Motivation for INF633/EE599
- 2- From 1µm to 45nm – the Moore law
  - The MOS transistor - limitations
  - Path to 45nm
- 3- From 45nm to 10nm – 3D transistors
- 4- From 10nm to 1nm – Nanotubes
- 5- 3D integration – Stacking silicon together

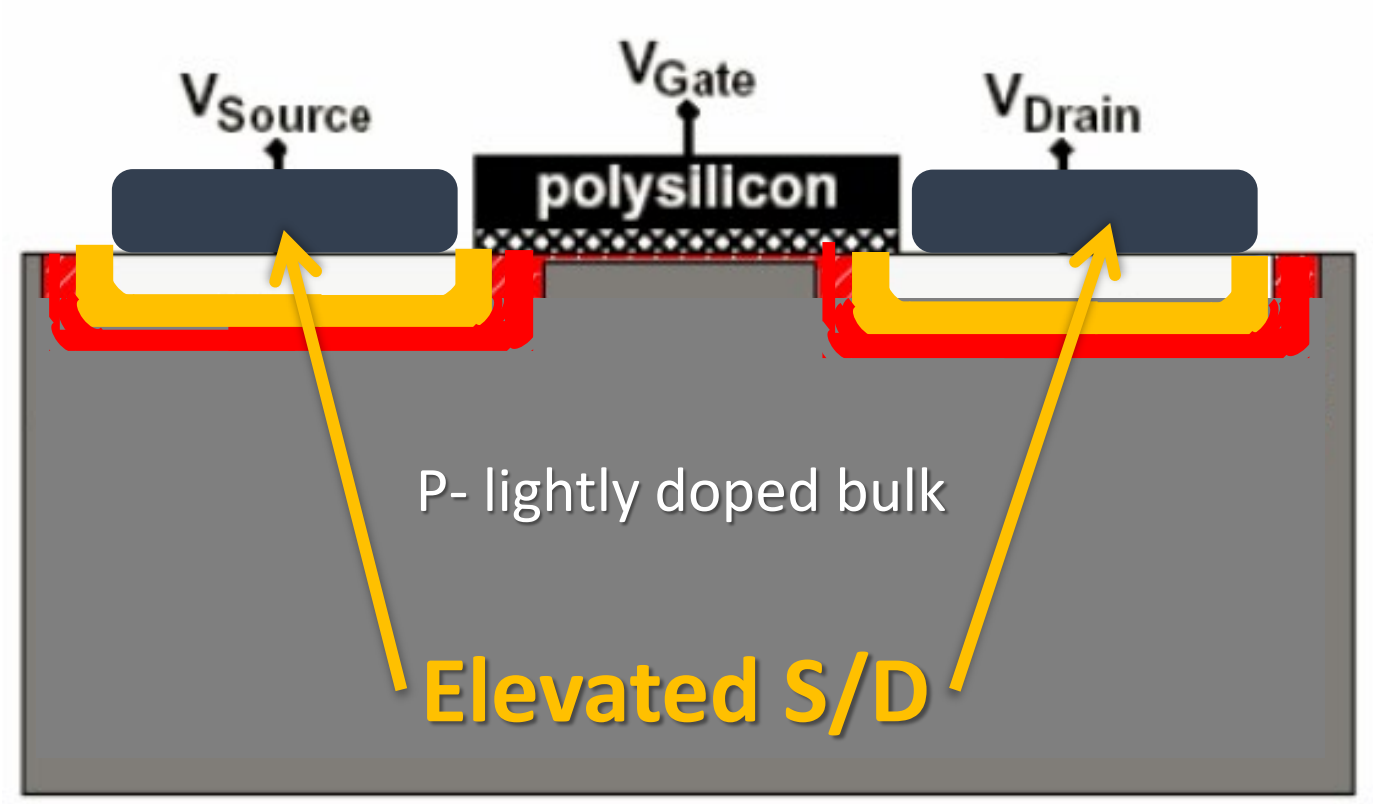
Remedies for size reduction: Pocket implant

- S/D engineering
- Lateral diffusion & angle implant



Remedies for size reduction: Elevated Source/Drain

- Selective epitaxy
- Planar structures



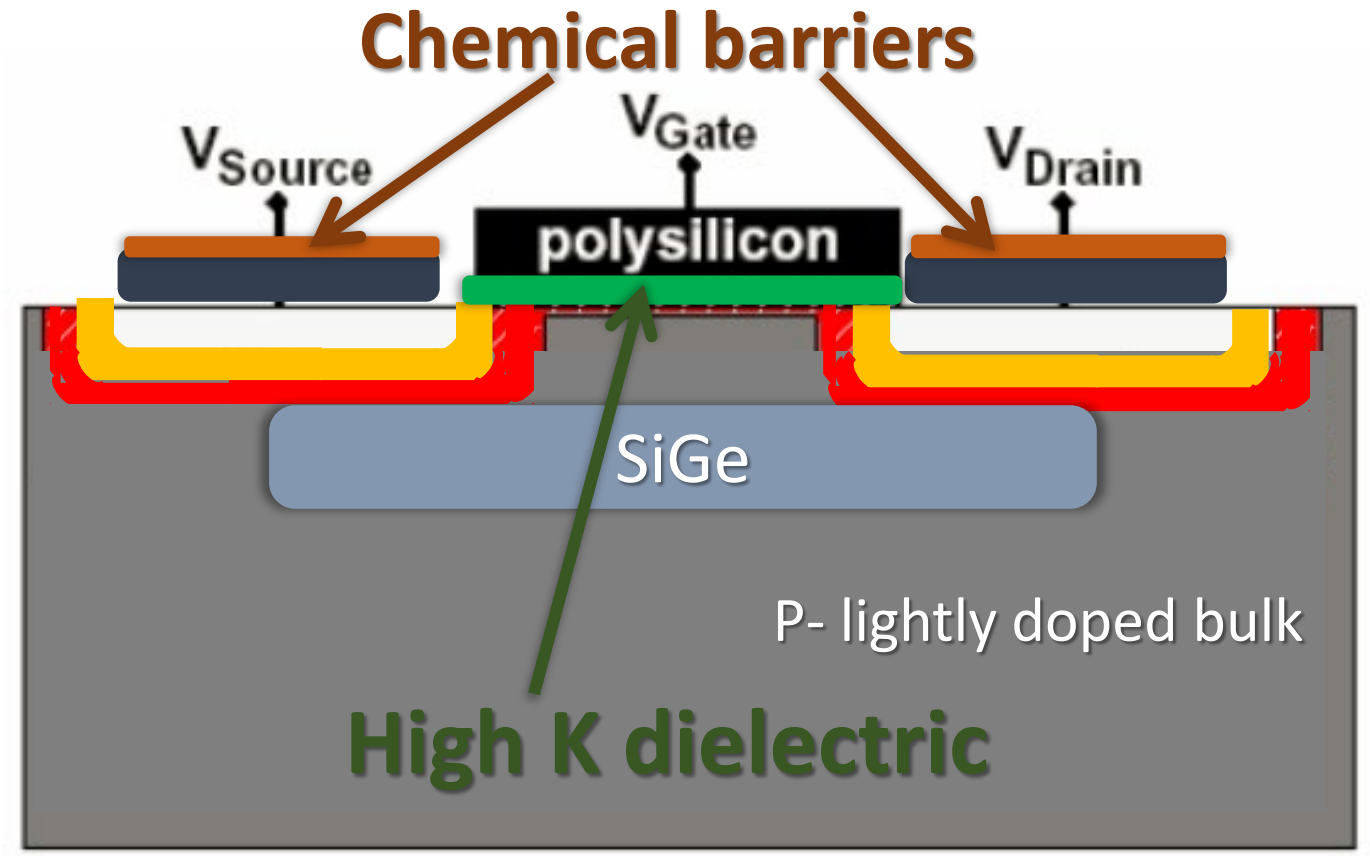
Other Remedies for size reduction:

Gate engineering SiO2 ➔ TaO2 ➔ HfO ➔ LaLuO3

K=4 ➔ K=10 ➔ K=22 ➔ K=40

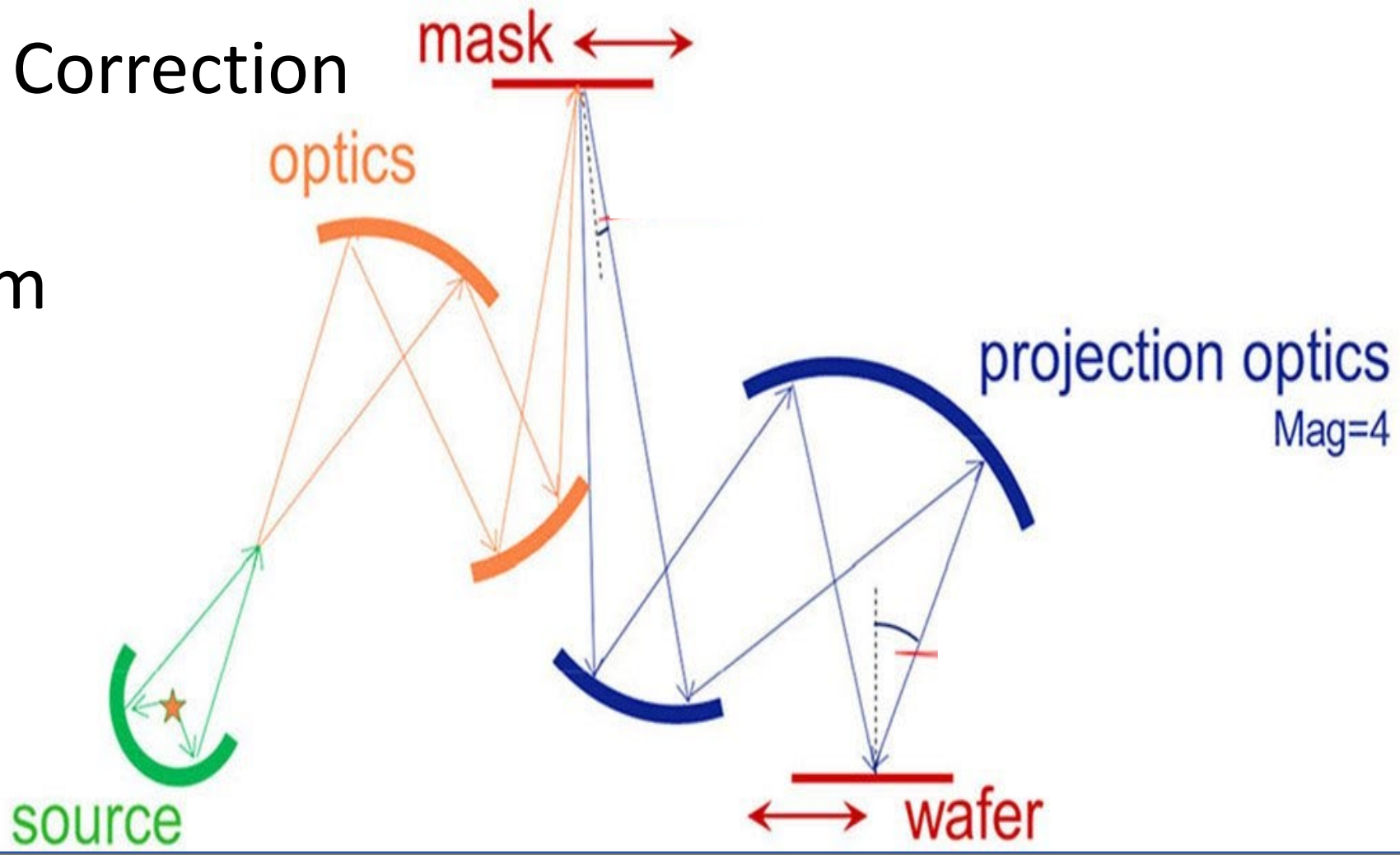
Chemical Barriers Silicides/Cu-platting/Dual Damazine

Deep UVs Visible 300-400nm ➔ G-line 436nm/I-Line 365nm ➔ Deep UV 193nm ➔ Extreme UV 13nm ➔ X-Ray 1nm



Advanced lithography for size reduction

- ➔Visible light 300-400nm
- ➔G-line 436nm/I-Line 365nm
- ➔Optical Proximity Correction
- ➔Deep UV 193nm
- ➔ Extreme UV 13nm
- ➔ X-Ray 1nm



Remedies for Size Reduction

- Pocket Implant
  - S/D engineering
  - Lateral diffusion & angle implant
- Elevated Source/Drain
  - Selective epitaxy
  - Planar structures
- Strained channel
  - SiGe or SC to relax the channel
  - 20% channel ➔ 100% higher mobility
- Gate engineering
  - SiO_2 ➔ TaO_2 ➔ HfO ➔ $LaLuO_3$
  - K=4 ➔ K=10 ➔ K=22 ➔ K=40
- Chemical Barriers
  - Silicides/Cu-platting/Dual damasime
- Ultra deep UVs
  - Visible 300-400nm ➔ G-line (436nm)/I-Line (365nm) ➔ Deep UV (193nm) ➔ Extreme UV (13nm) ➔ X-Ray (1nm)

NORTHERN ARIZONA UNIVERSITY

1 From Micro to Nano-electronics

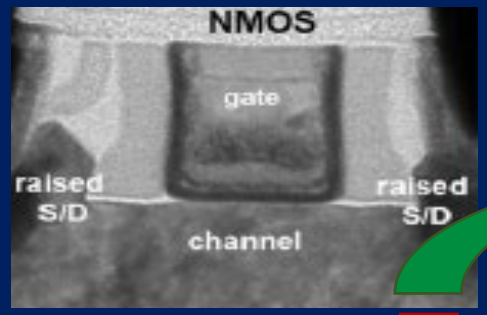
- 1- Motivation for INF633/EE599
- 2- From 1µm to 45nm – the Moore law
  - The MOS transistor - limitations
  - Path to 45nm
- 3- From 45nm to 10nm – 3D transistors
- 4- From 10nm to 1nm – Nanotubes
- 5- 3D integration – Stacking silicon together

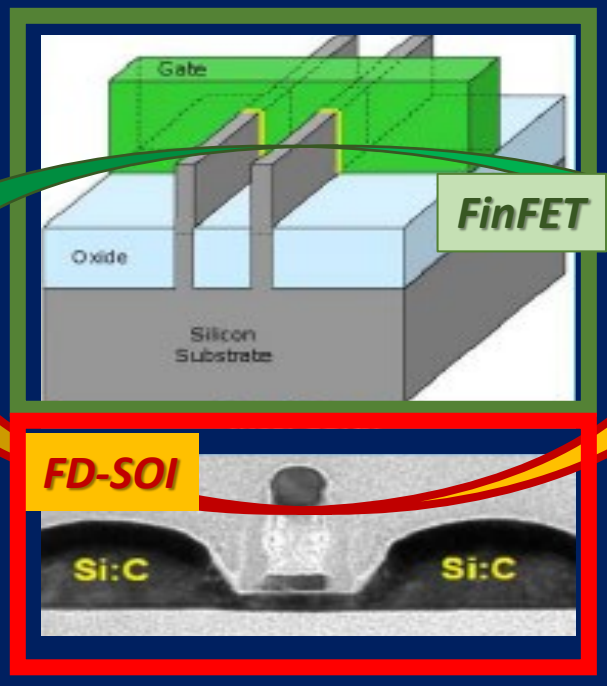
MOSFET EVOLUTION to 10nm: FinFET vs FD-SOI

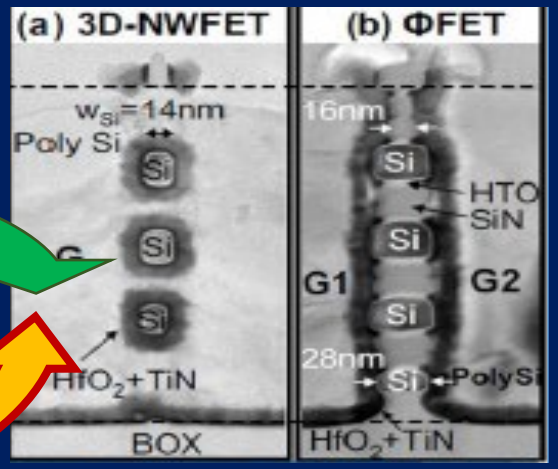
32/28 nm planar

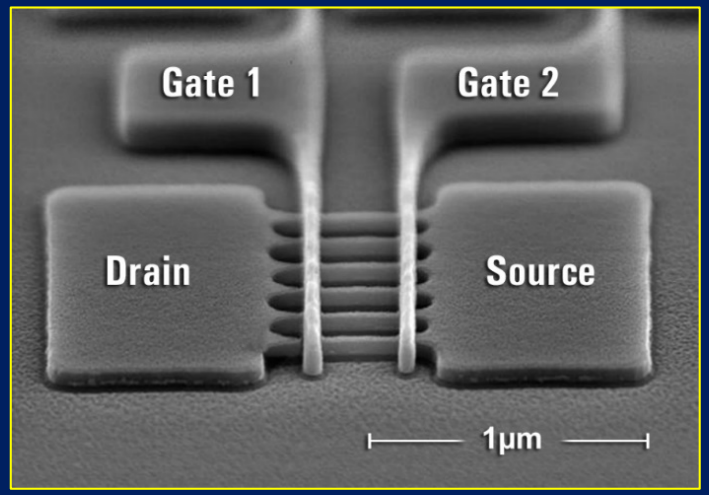
22/10nm thin body

10nm to 1nm









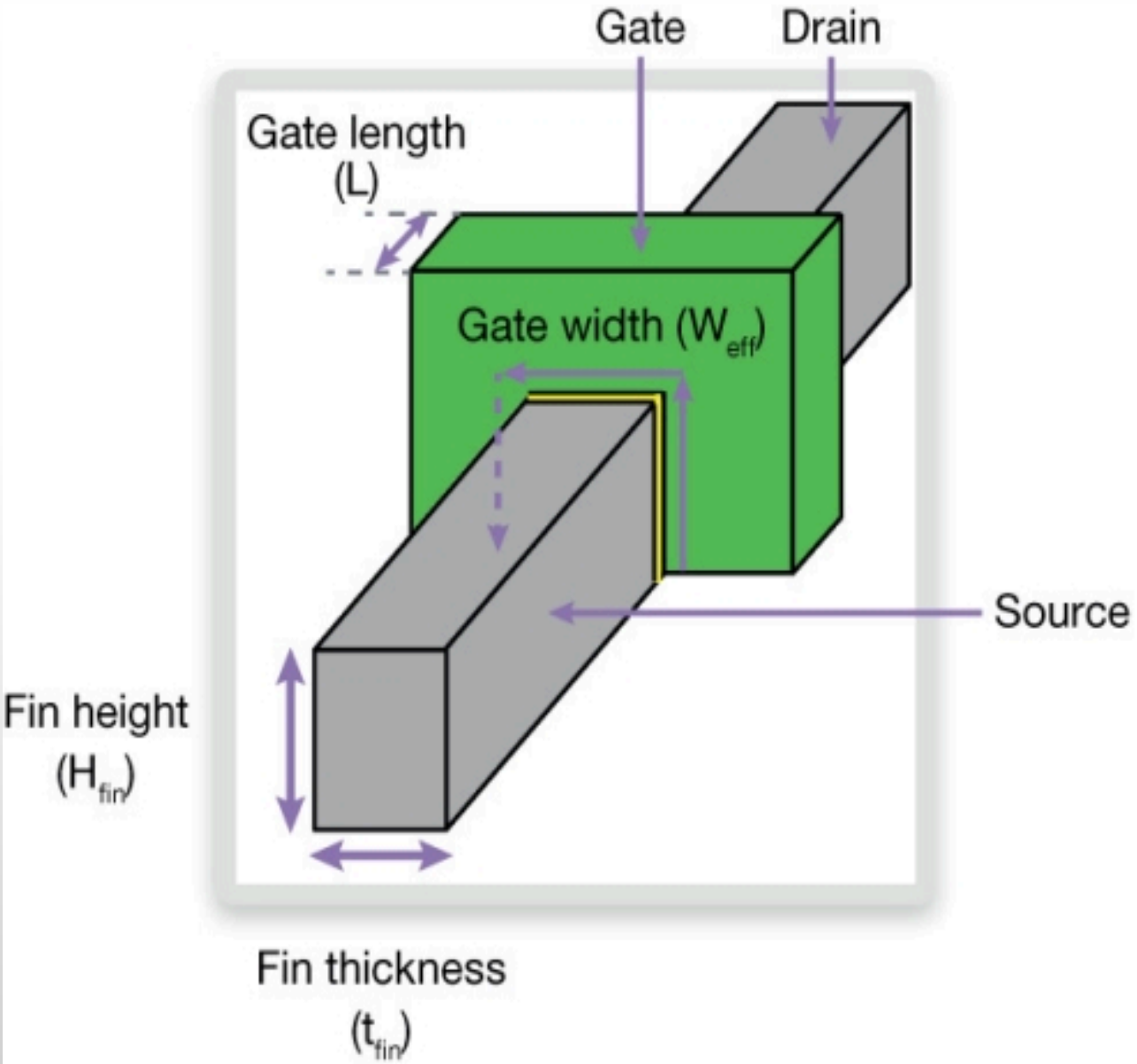
Pocket Implant
Elevated S/D
Strained silicon
Gate engineering

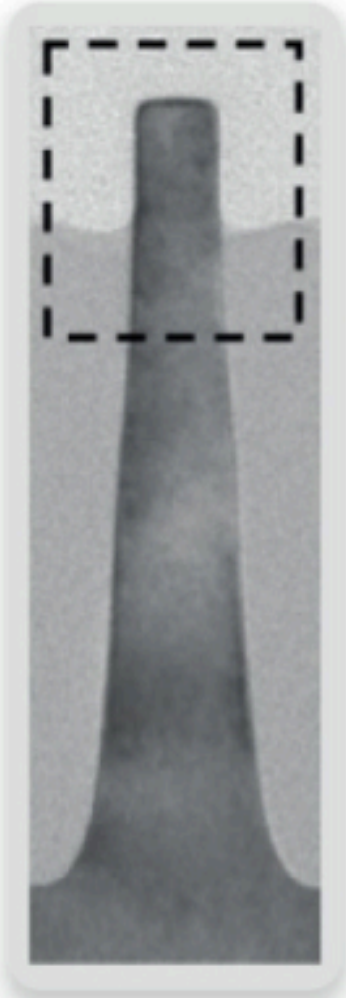
FinFET
3D gate
FD-SOI
Wafer bonding

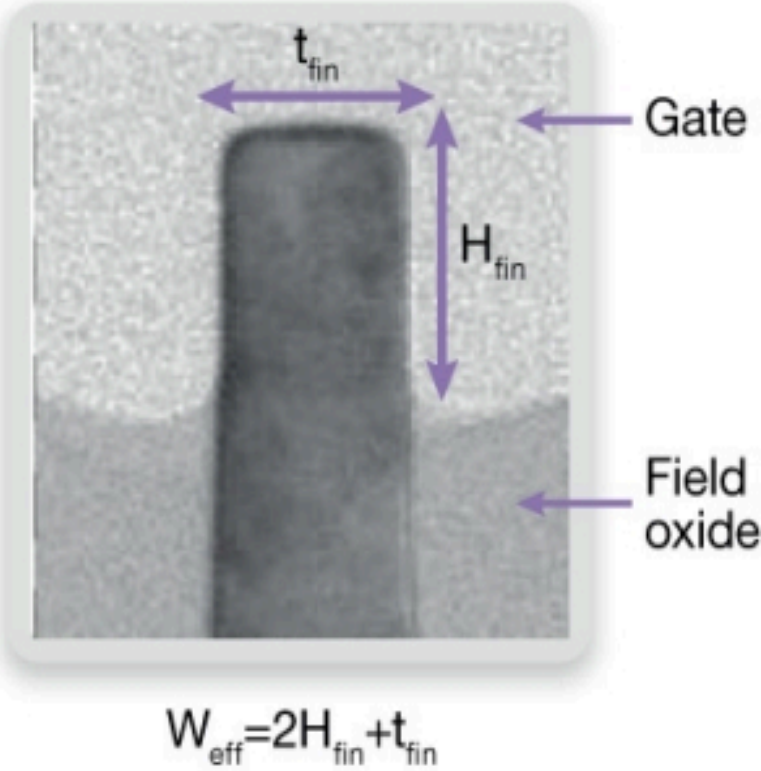
FinFET+SOI
Nanowires
Carbon
Wafer bonding

Example of FinFET

FinFET transistor





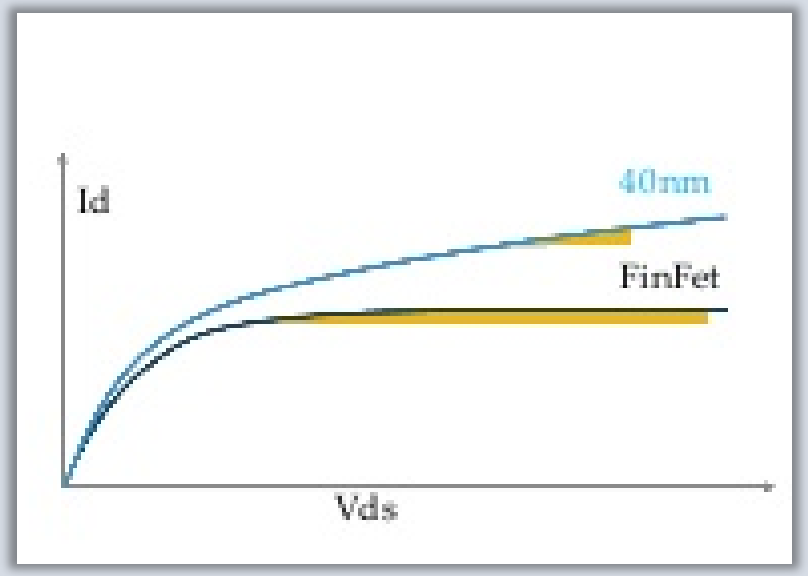


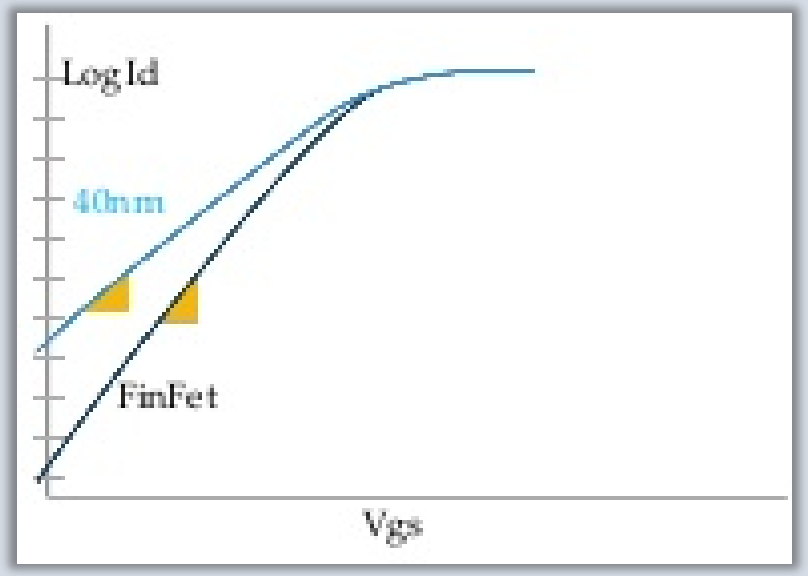
$W_{eff}=2H_{fin}+t_{fin}$

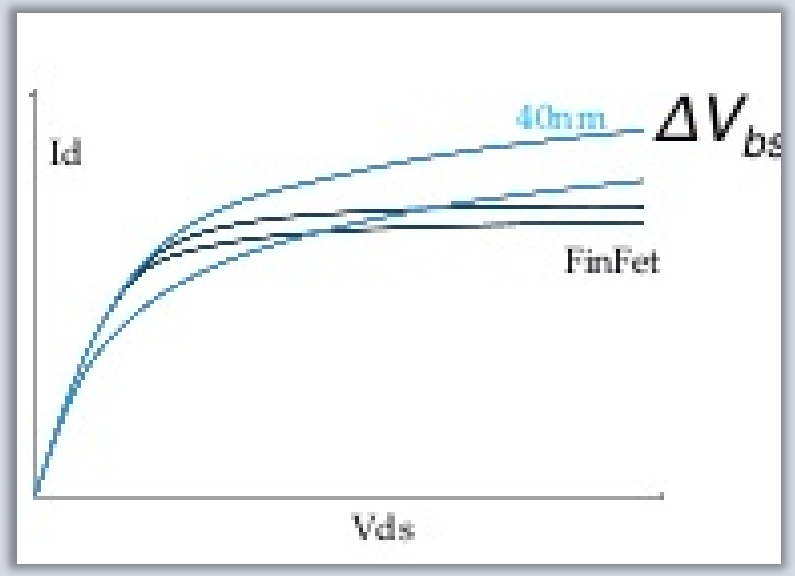
The benefits of FinFET

MOS device characteristics drastically improve

Compare 40nm planar structure to 40nm FinFET





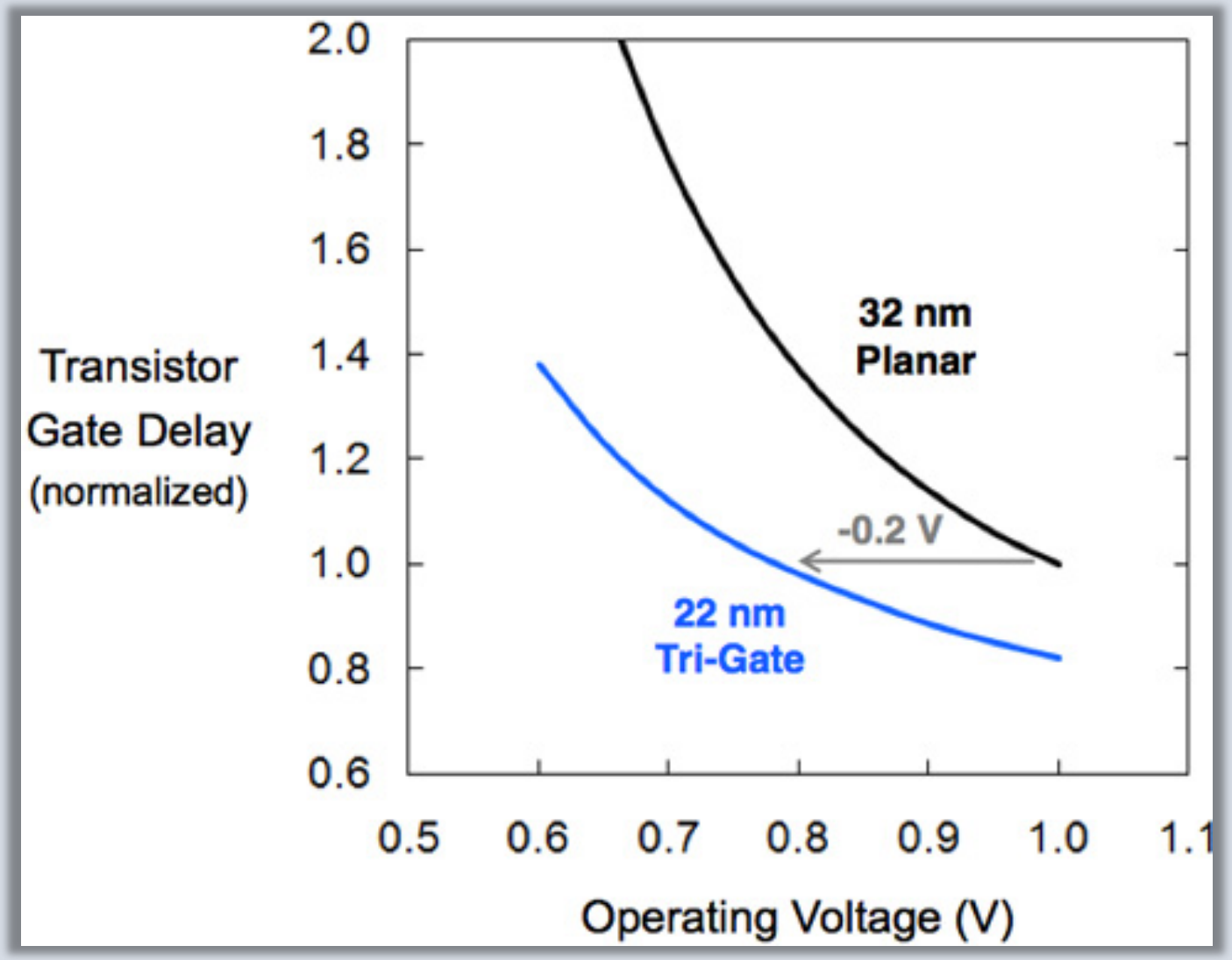


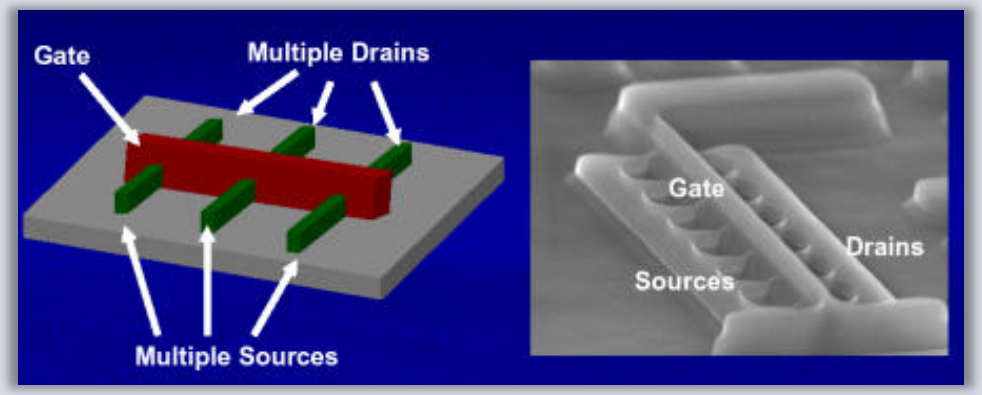
Early effect is much lower

Sub threshold slope is close to ideal

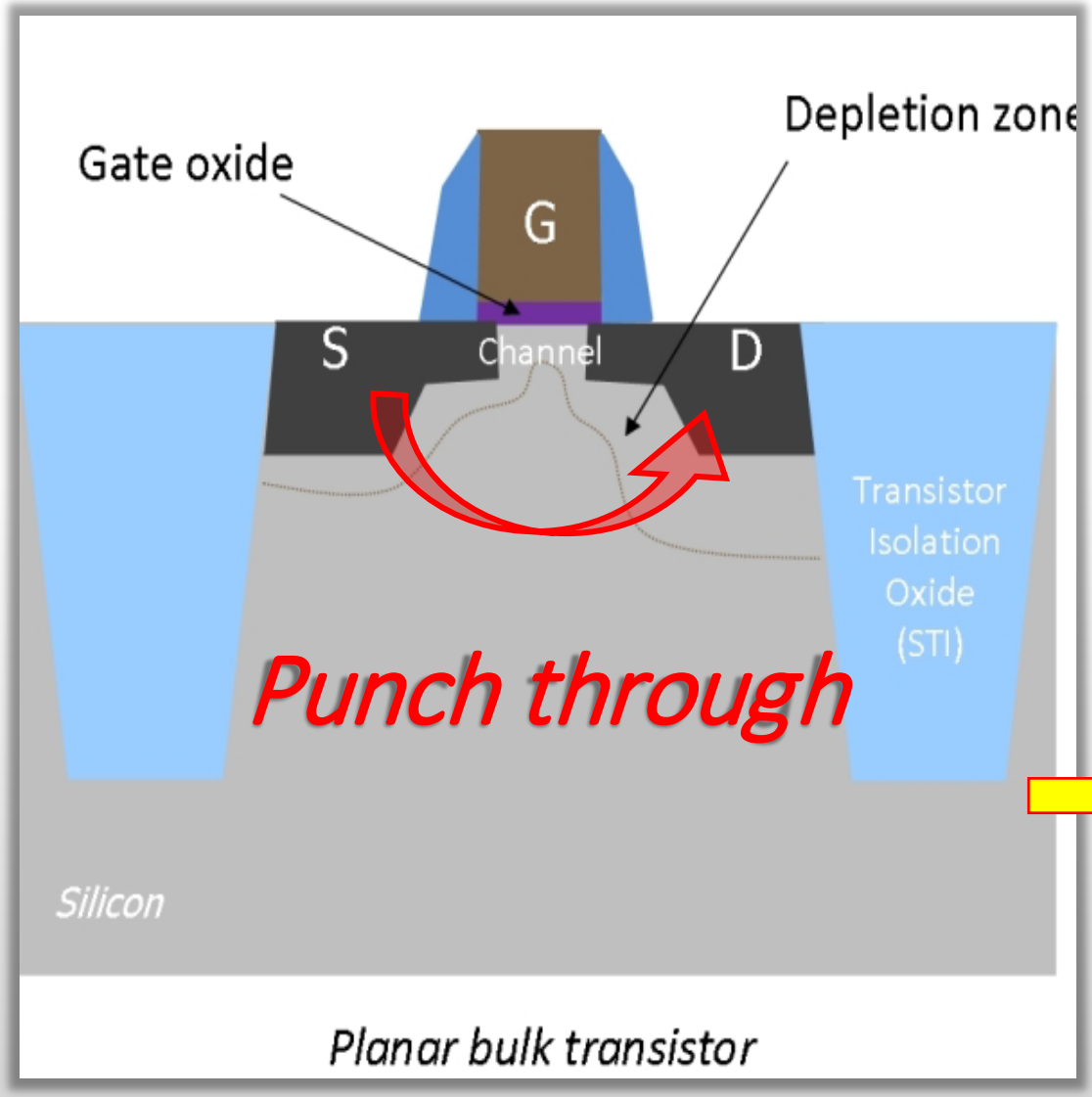
g_{bs} or body effect is much lower

The benefits of FinFET on transistor gate delay

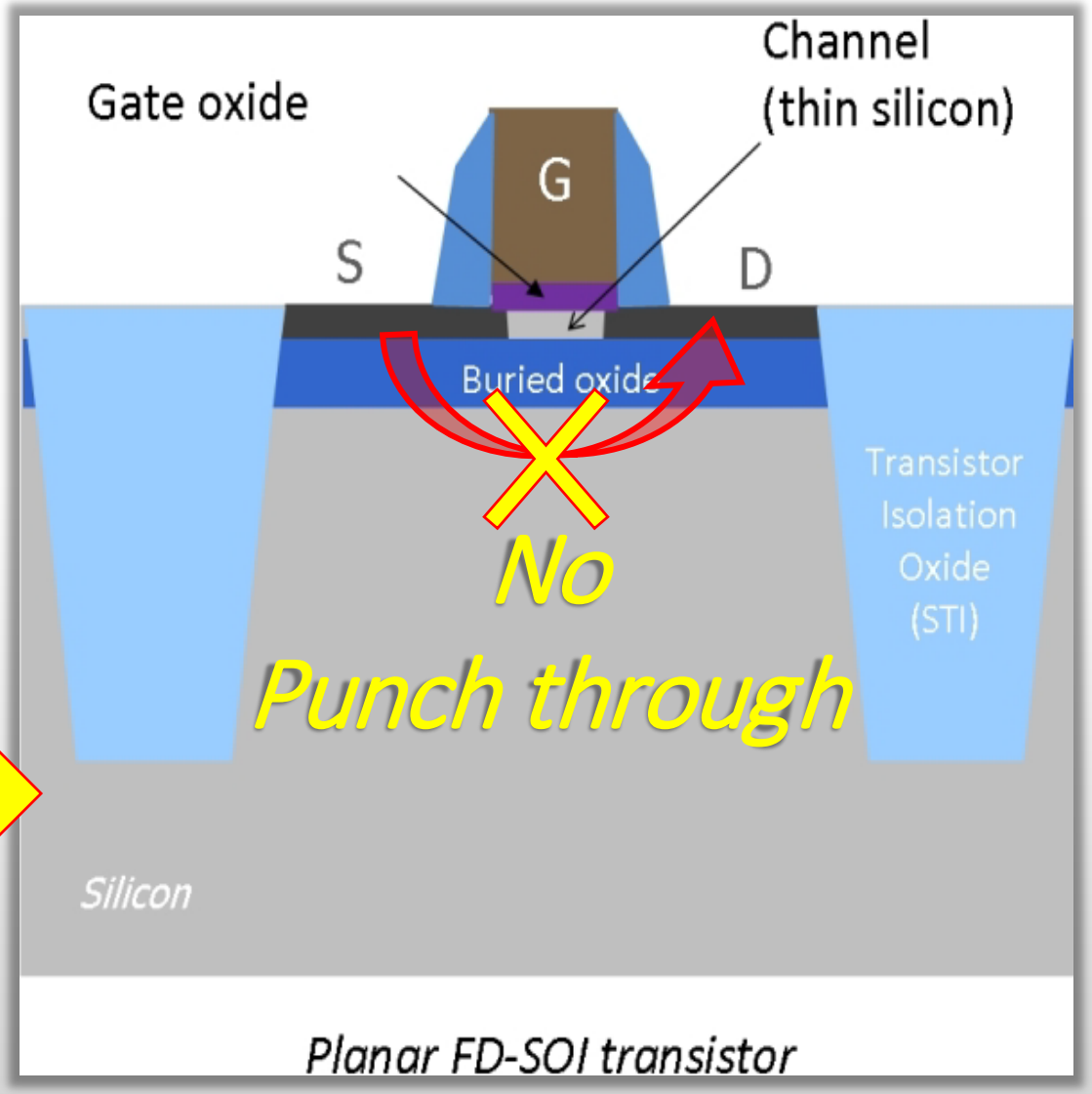




Fully Depleted Silicon on Insulator MOSFET Transistor

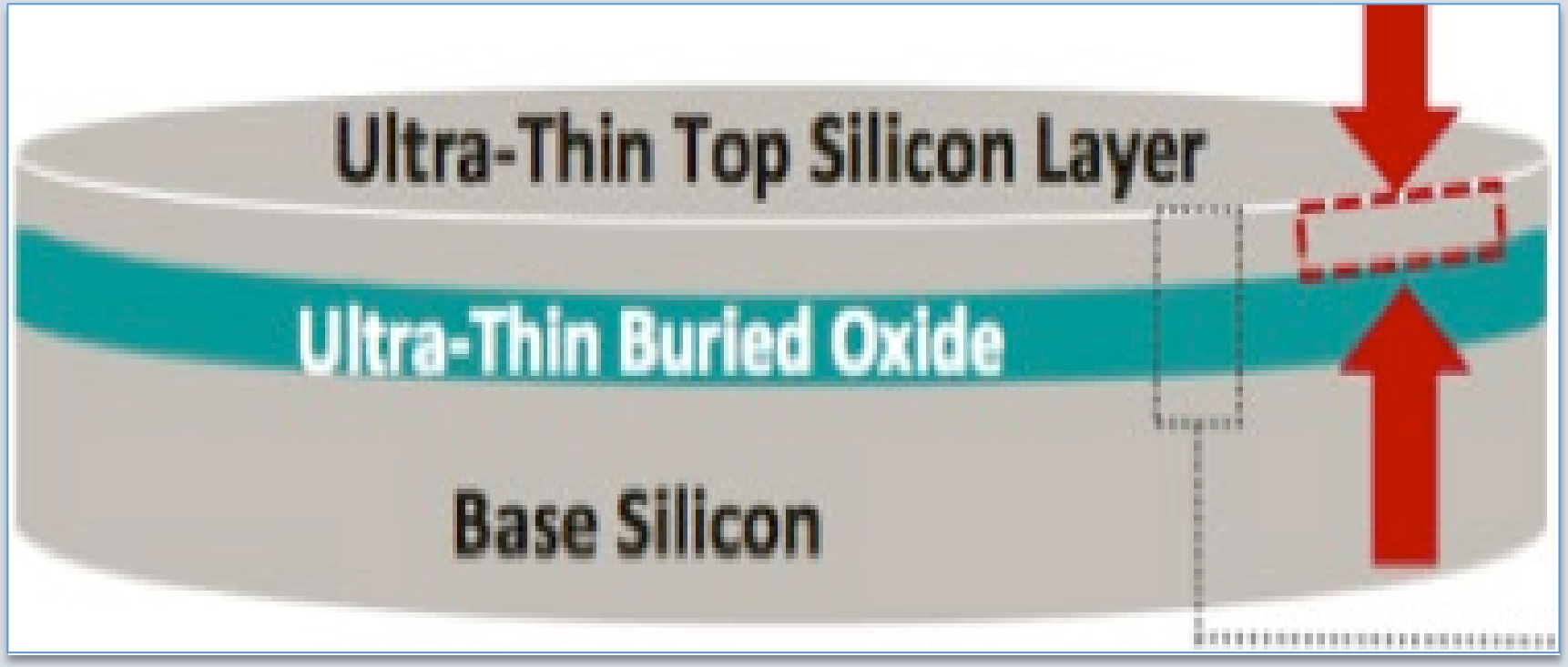


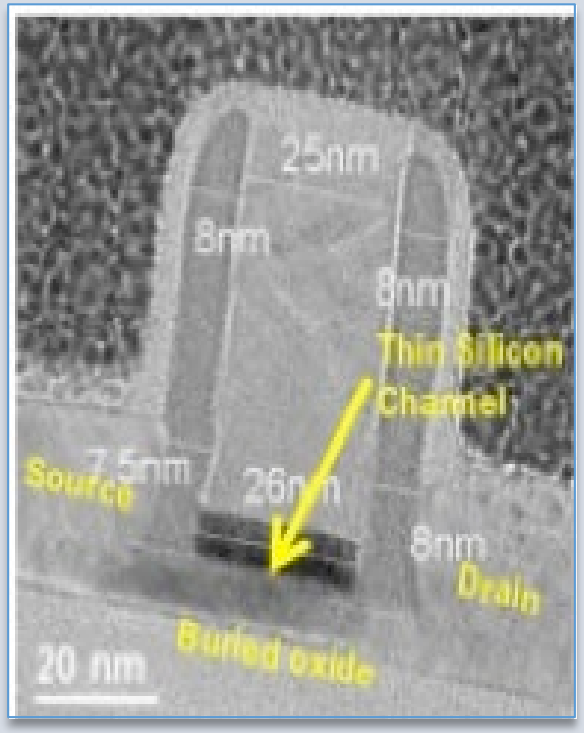
Planar bulk transistor



Planar FD-SOI transistor

Manufacturing of the FD-SOI transistors (SOITEC)

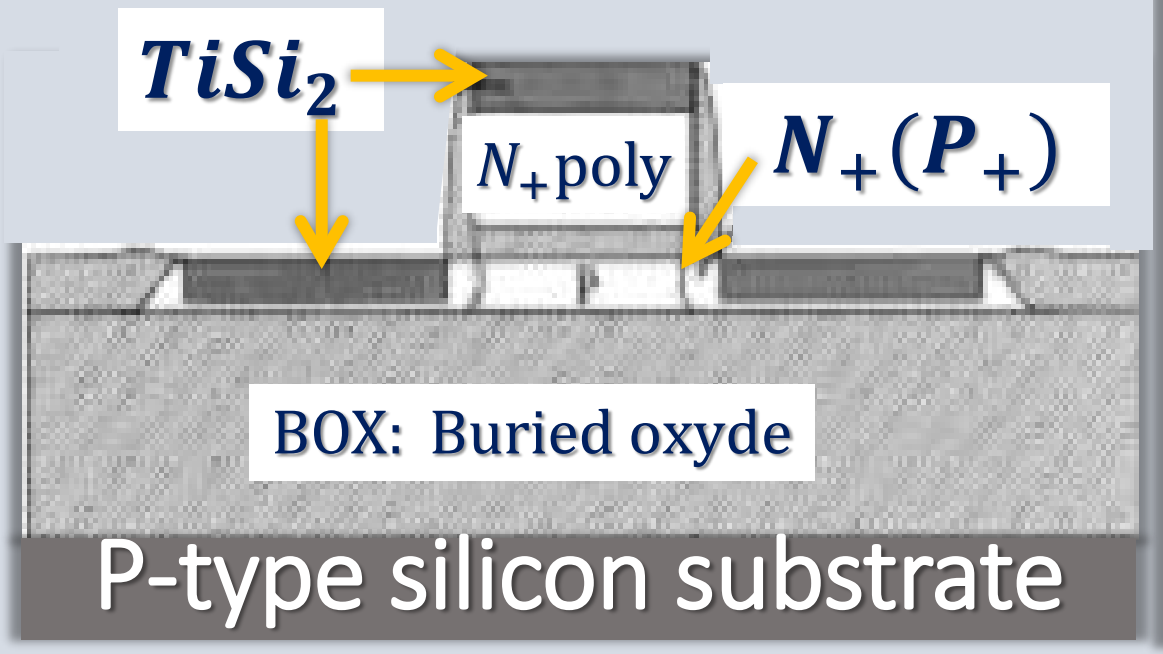


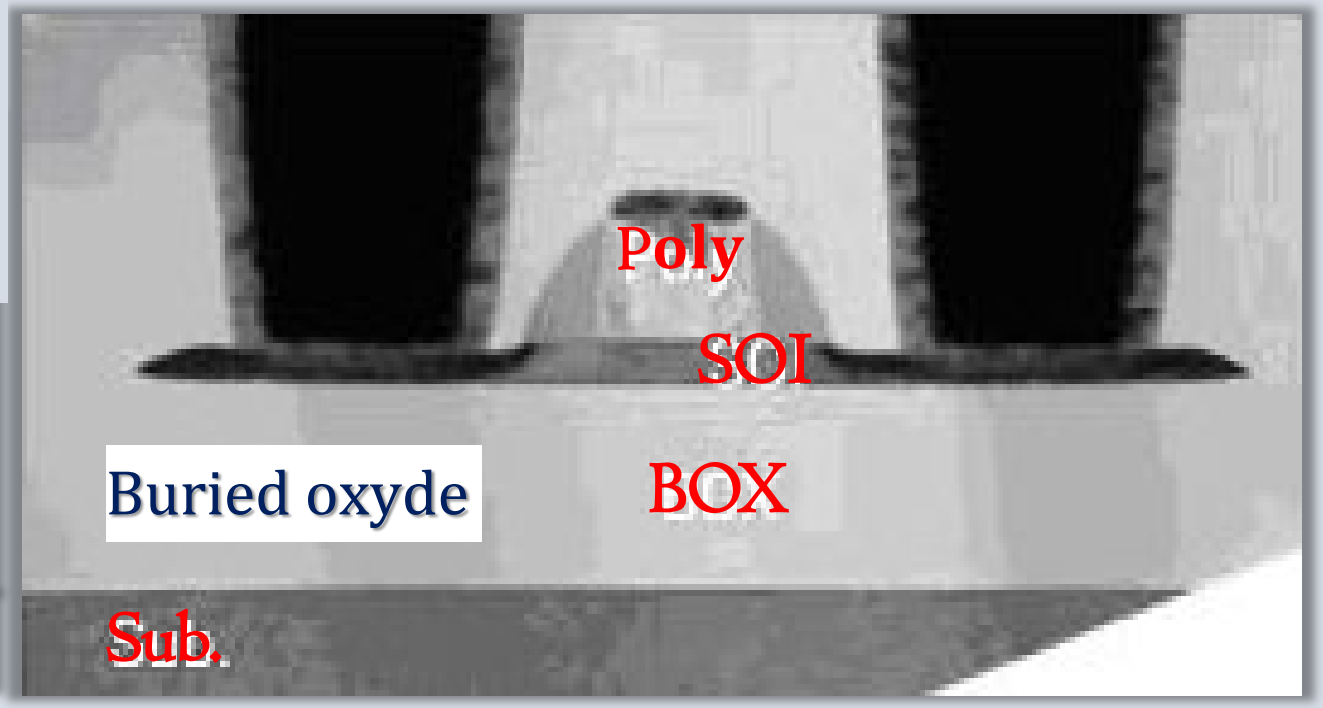


Raw wafers:
top silicon of 10nm
BOX of 20nm

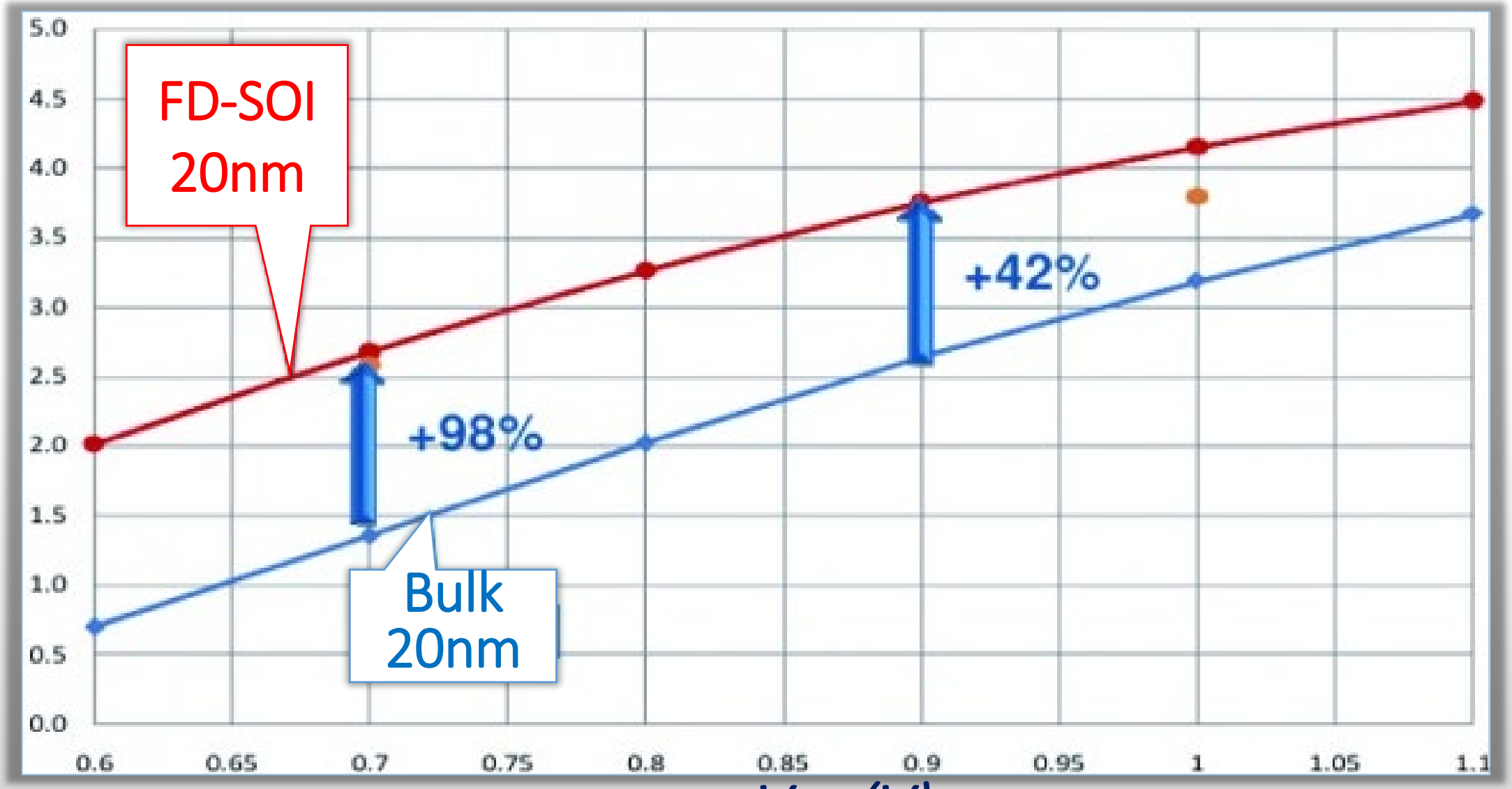
Final wafers:
top silicon of 5nm lost during fabrication

Example of SEM view FD-SOI

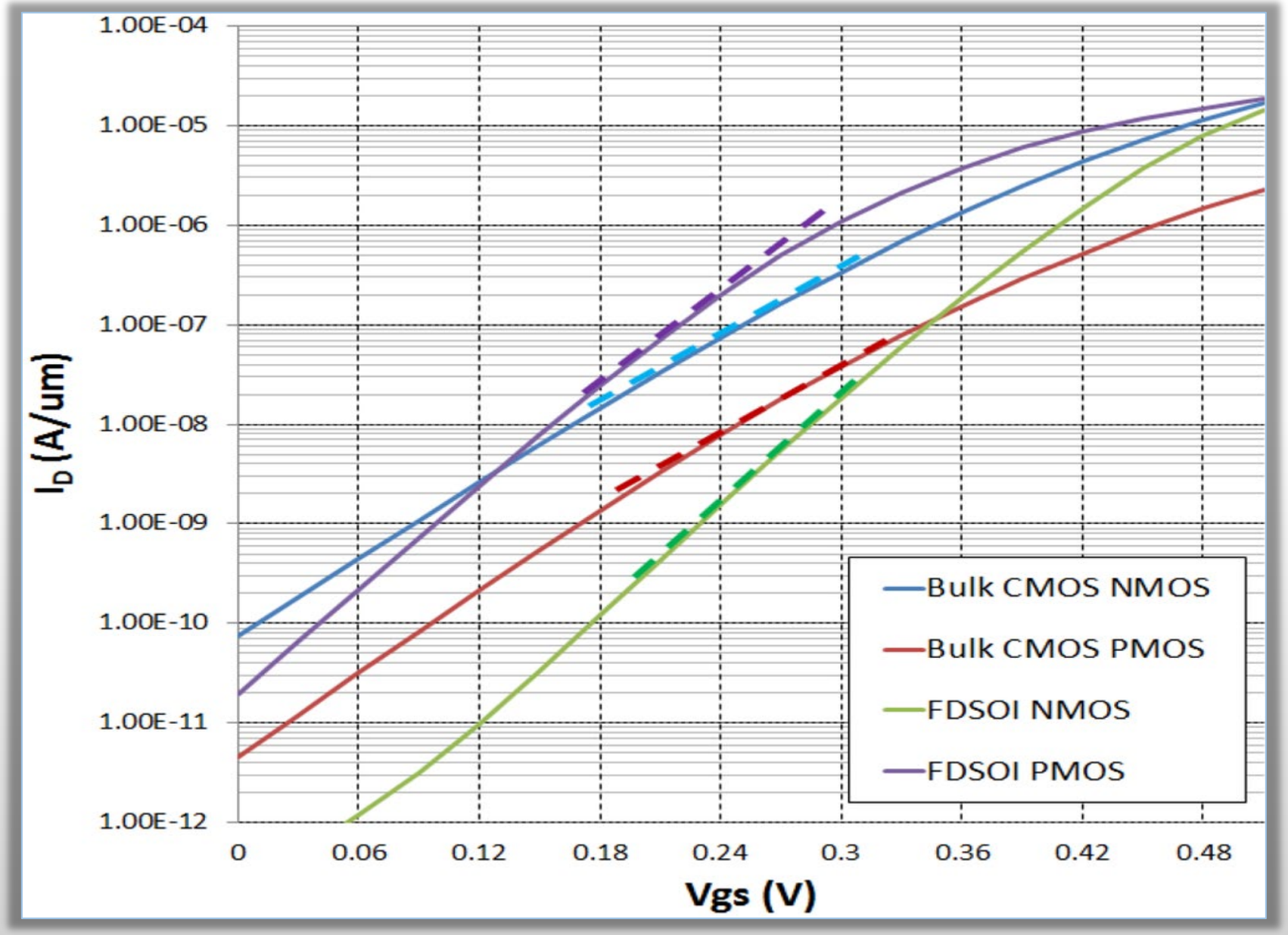




Effect of FD-SOI at low voltage



FD-SOI: Sub-Threshold Slope



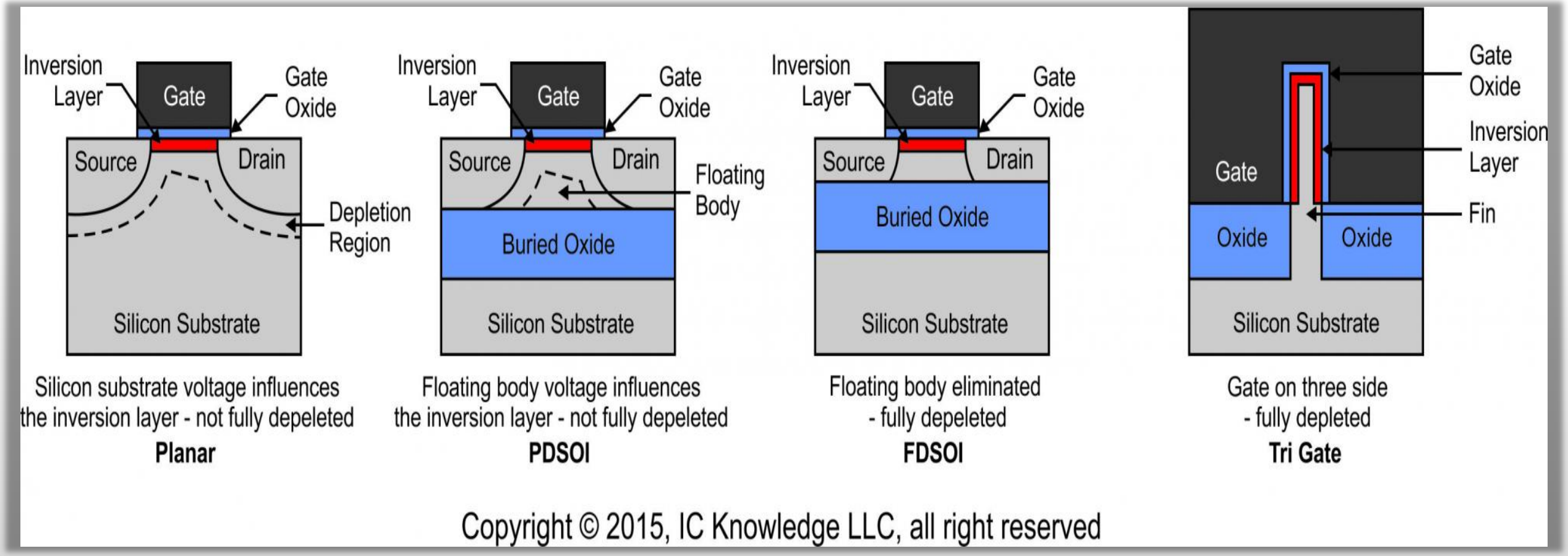
NORTHERN ARIZONA UNIVERSITY

1 From Micro to Nano-electronics

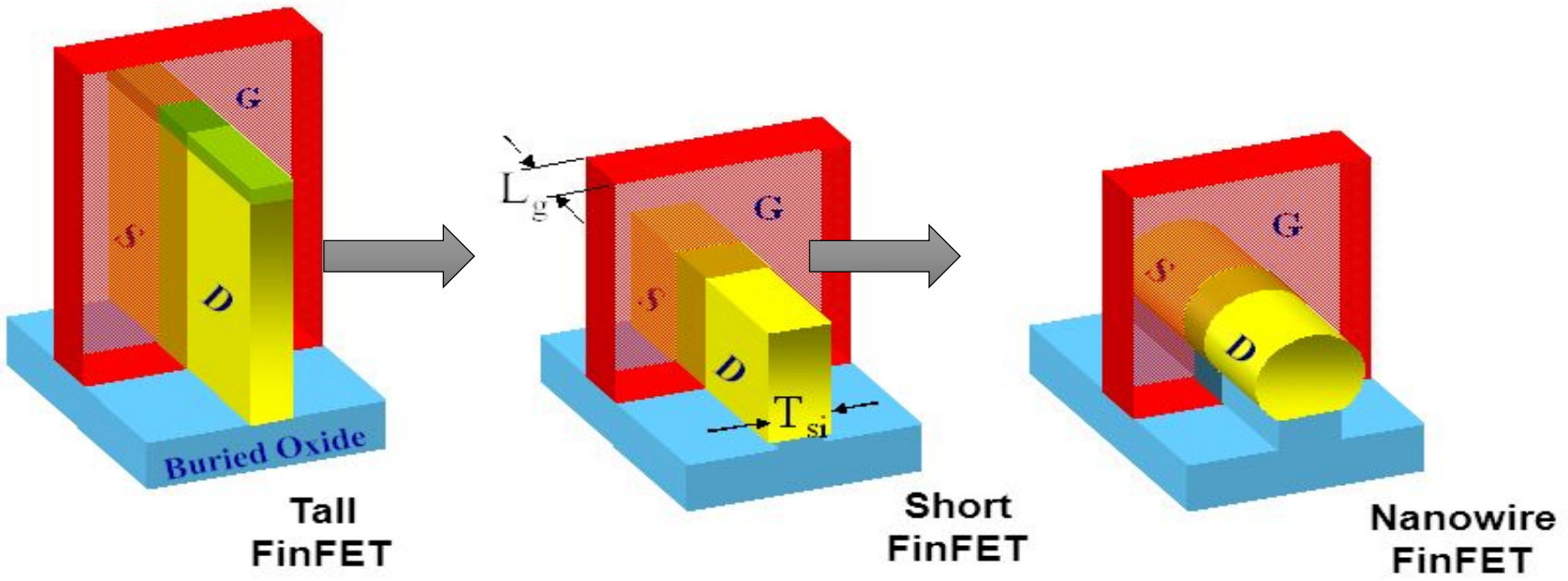
- 1- Motivation for INF633/EE599
- 2- From 1µm to 45nm – the Moore law
  - The MOS transistor - limitations
  - Path to 45nm
- 3- From 45nm to 10nm – 3D transistors
- 4- From 10nm to 1nm – Nanotubes
- 5- 3D integration – Stacking silicon together

Advanced Lithography roadmap of ASML (EEtimes Nov 3rd 2016)

Combine FD-SOI & Fin FET



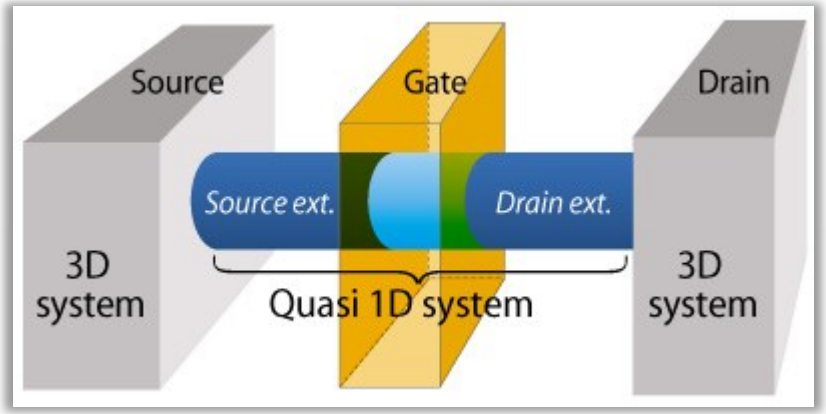
Path to nanowire FET

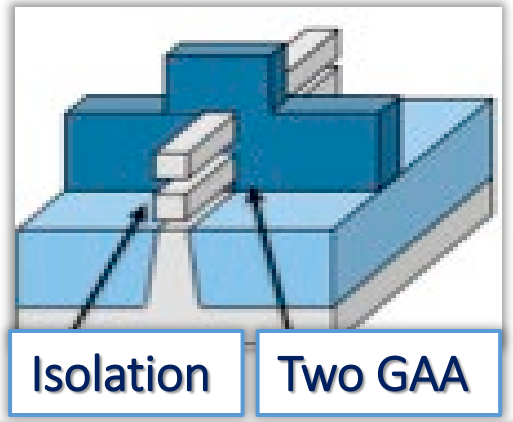


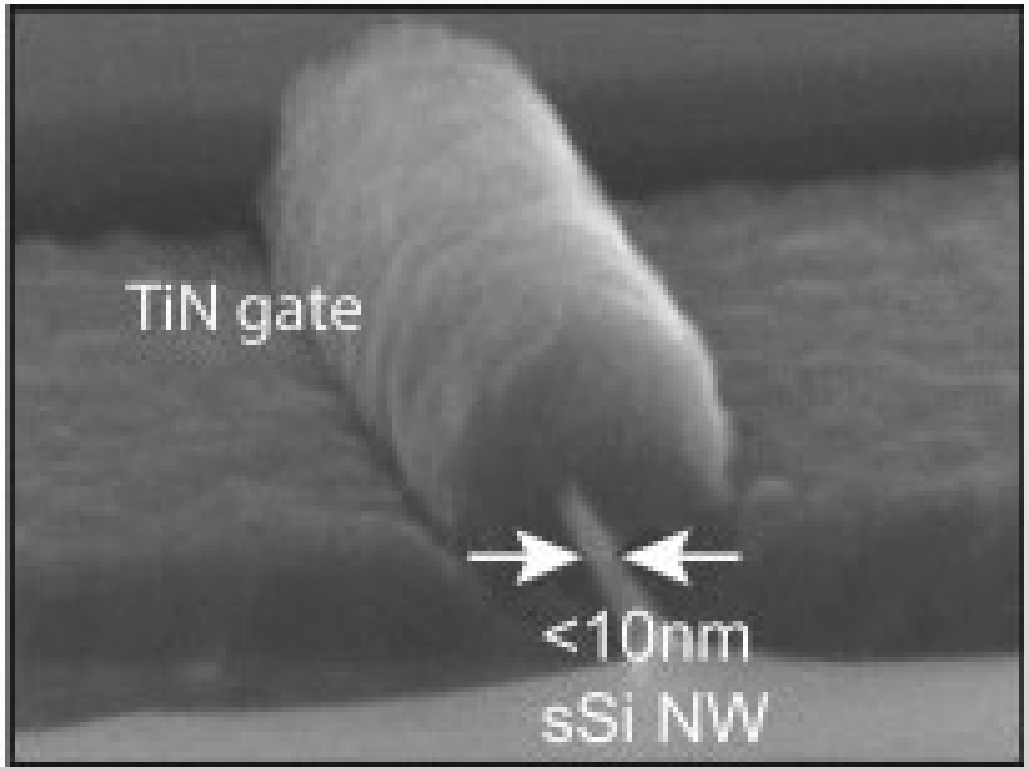
- **Tall FinFET** has the advantage of providing a large W and therefore large I_{on} while occupying a small footprint.
- **Short FinFET** has the advantage of less challenging lithography and etching.
- **Nanowire FinFET** gives the gate even more control over the silicon wire by surrounding it.

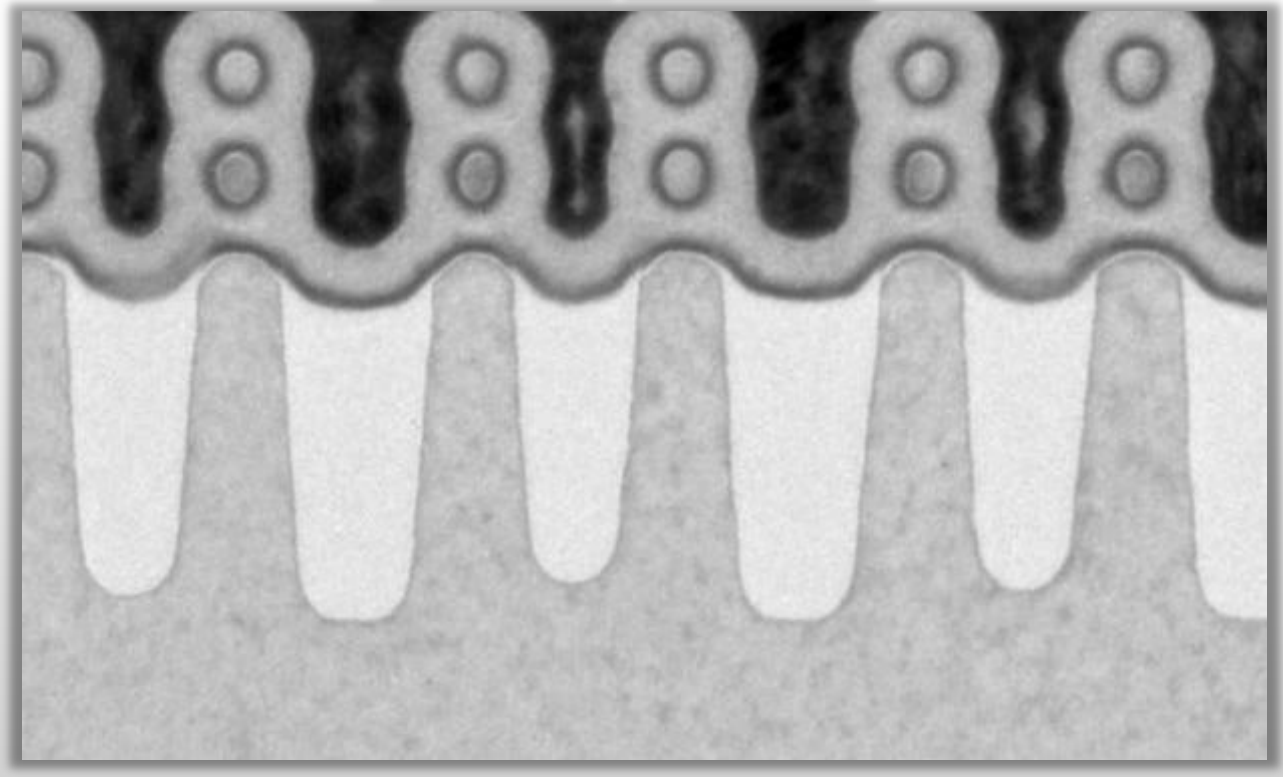
C. Hu

Gate All Around (GAA)

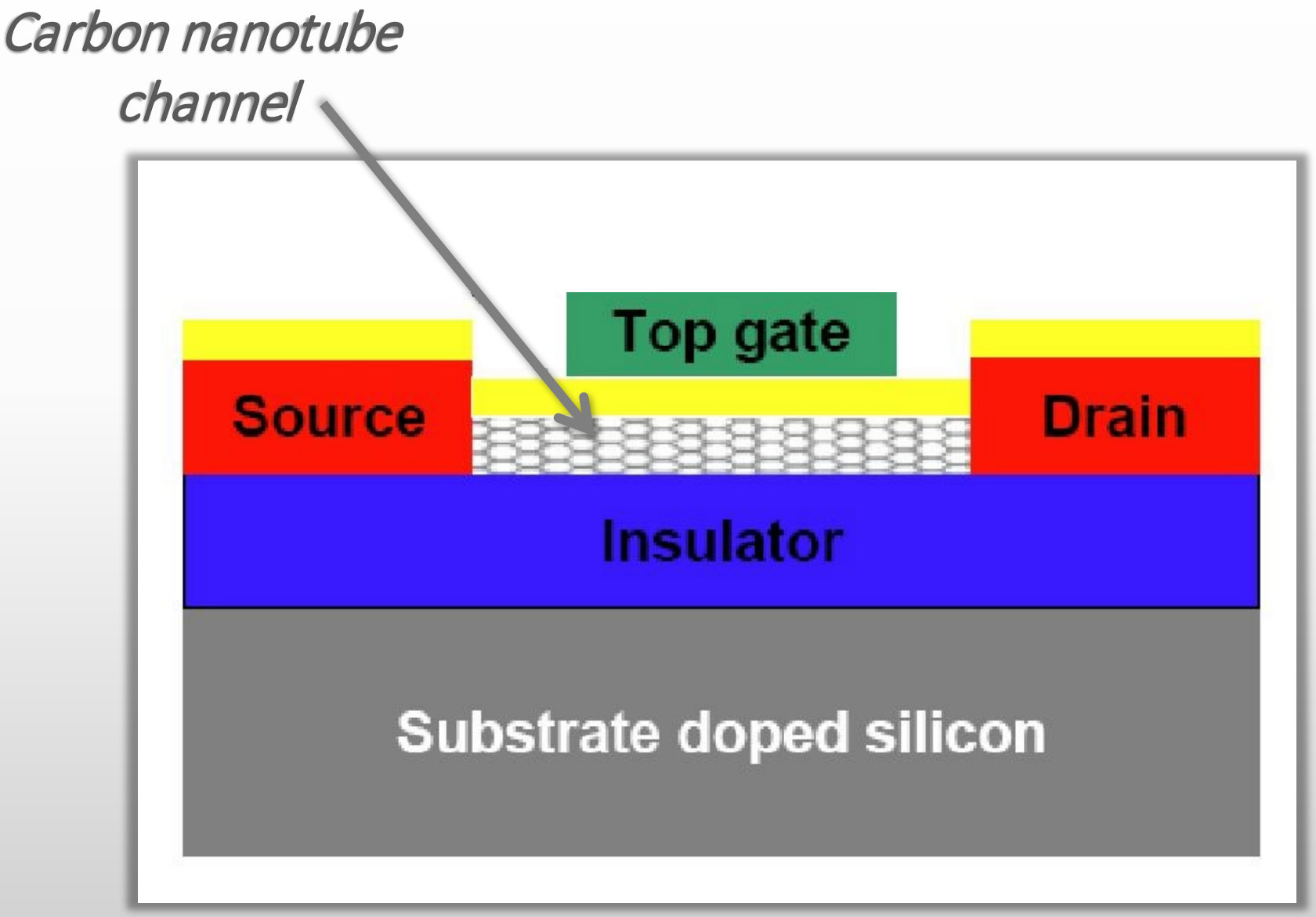




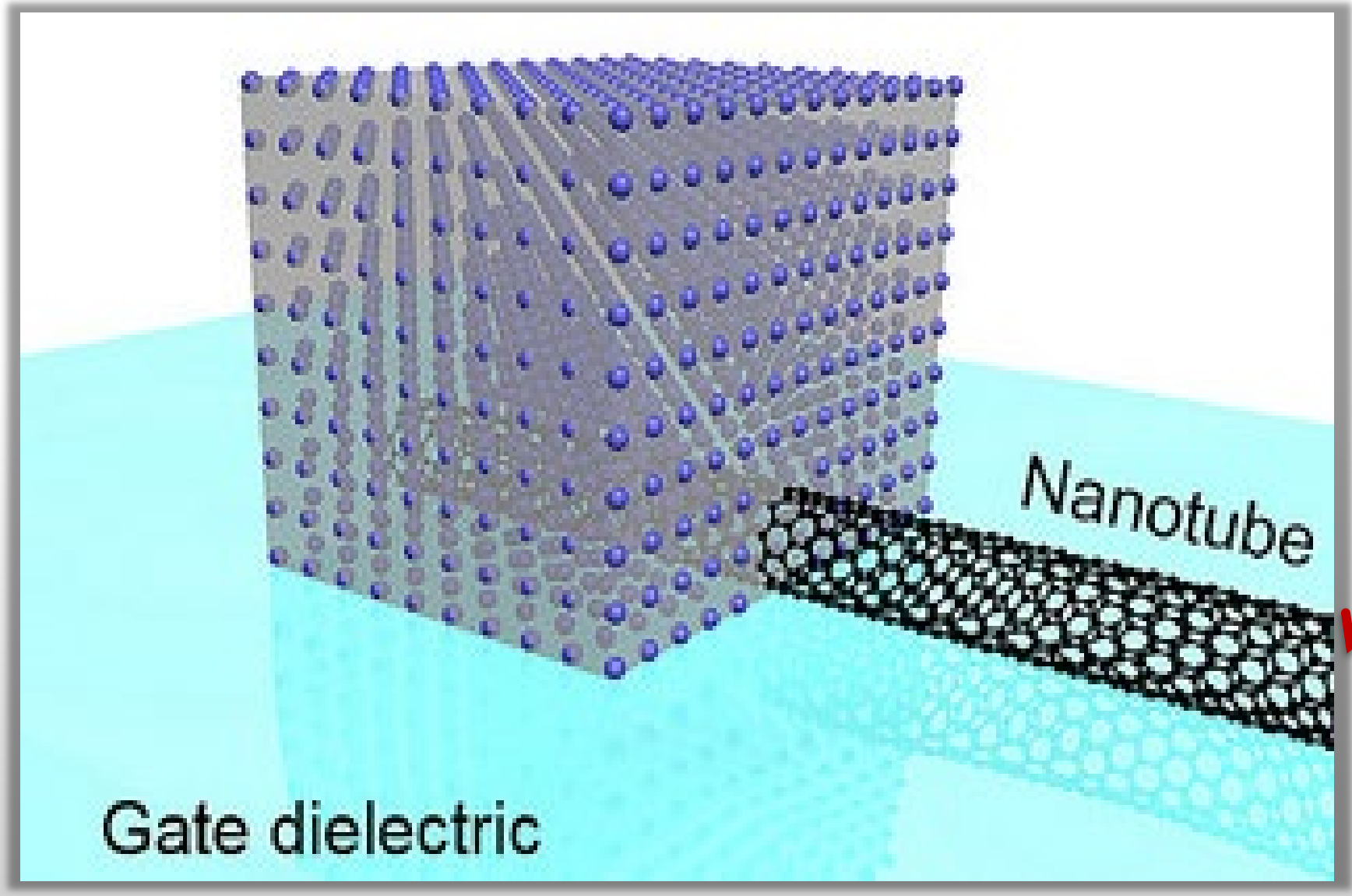




Carbon Nanotube FET

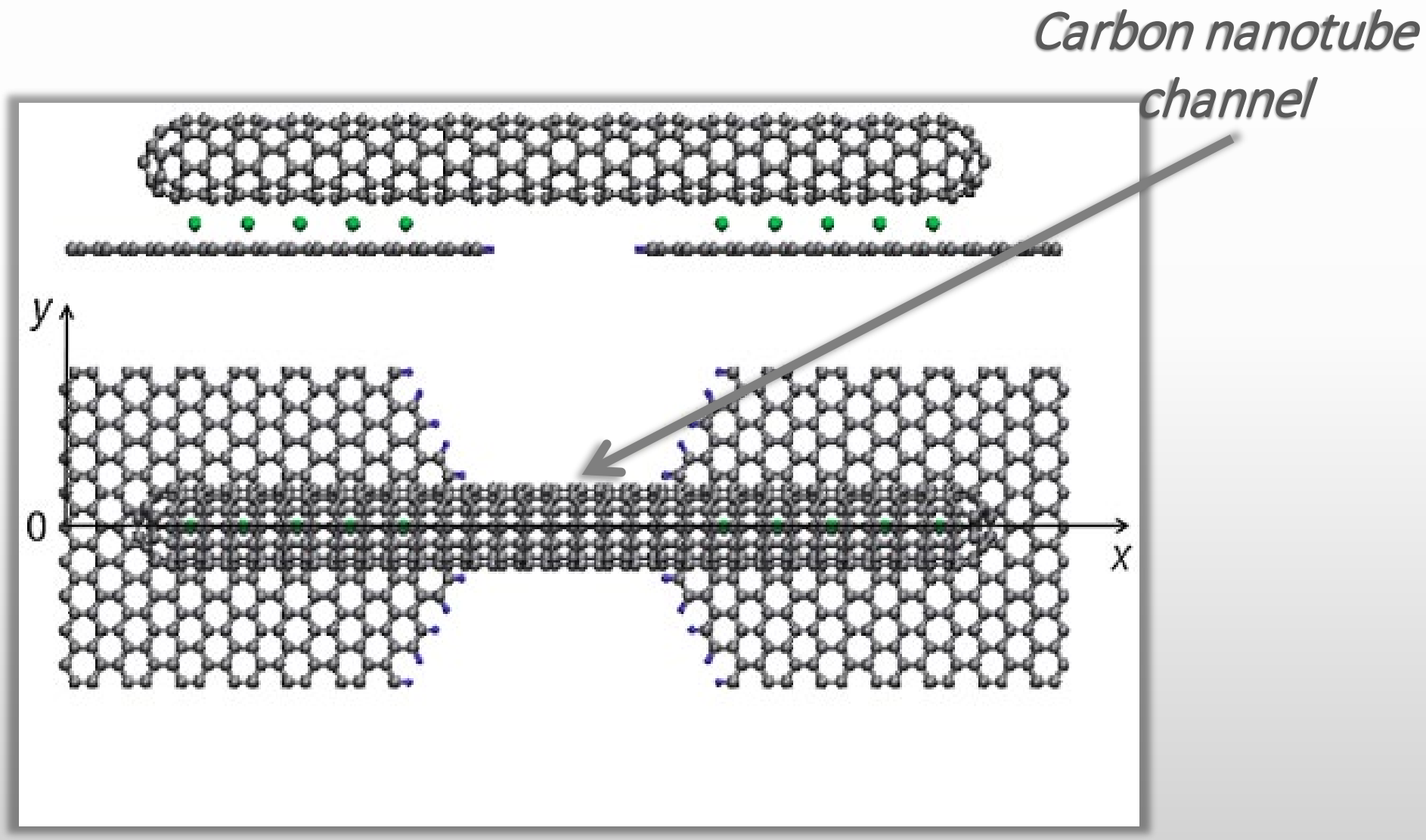


Carbon Nanotube FET: Molecular models

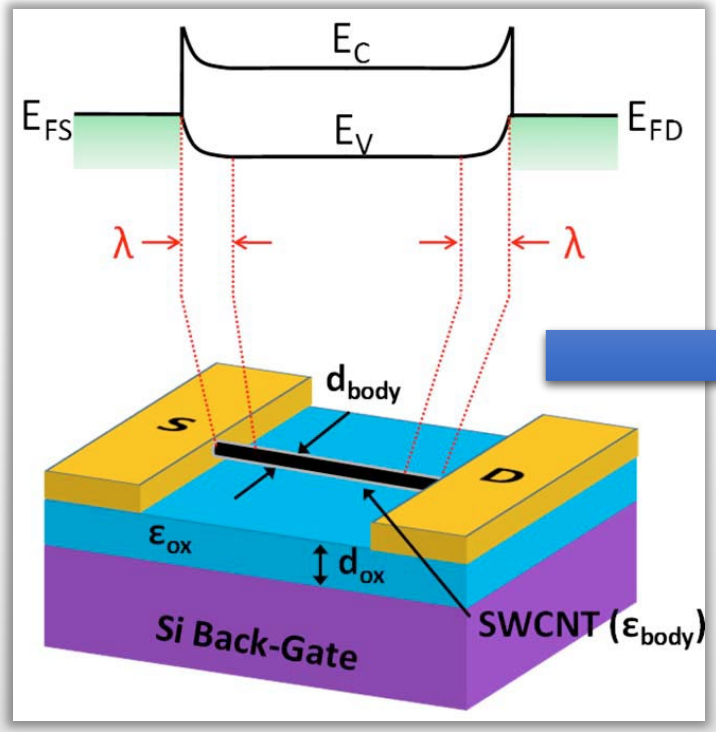


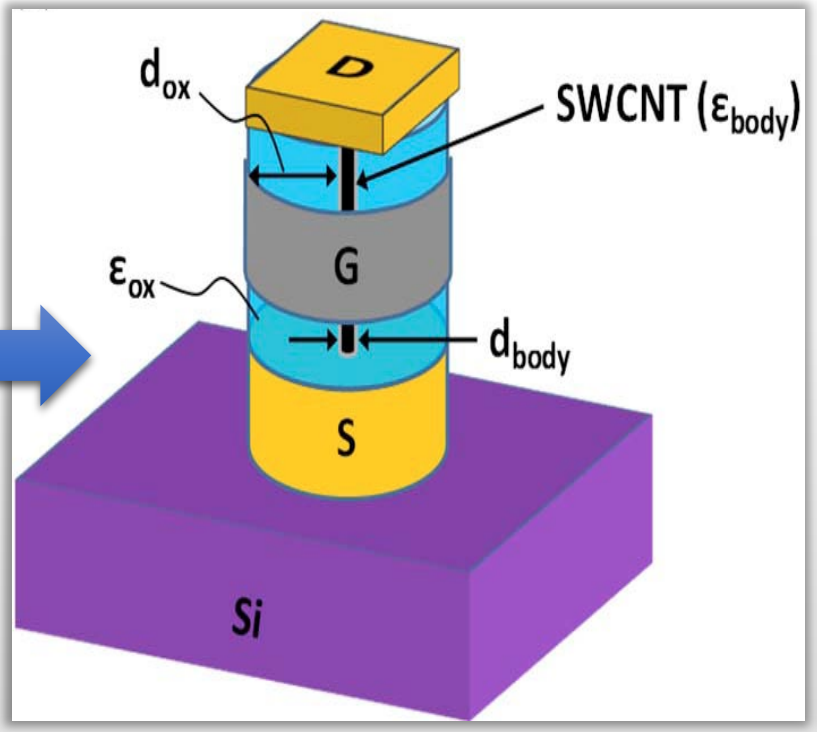
Carbon nanotube channel

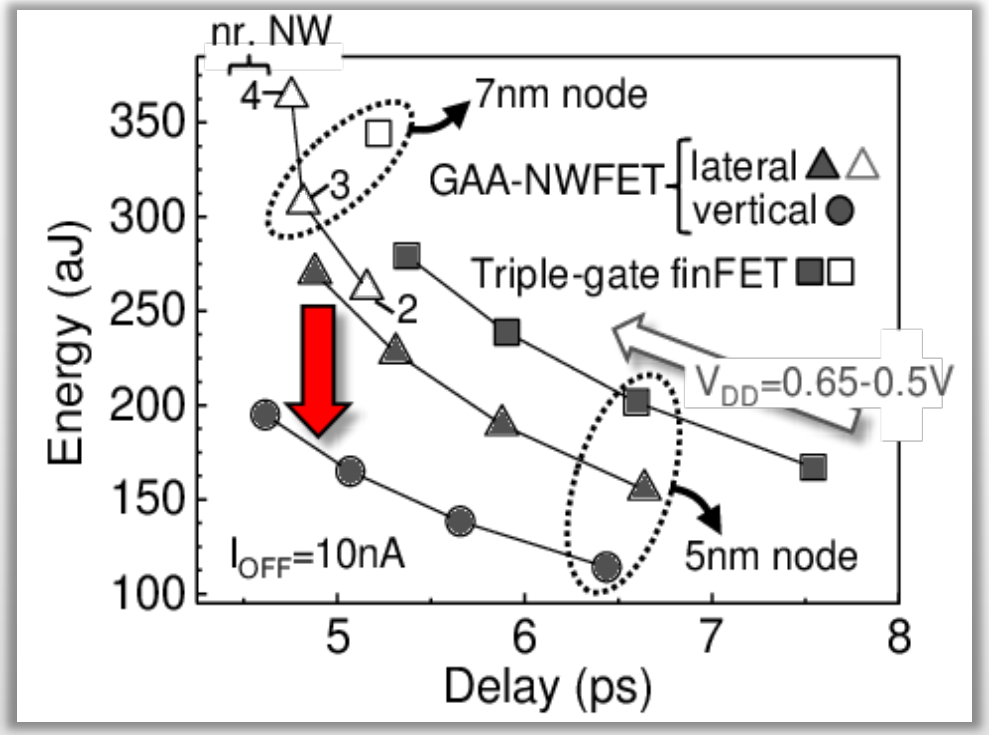
Carbon Nanotube FET: Molecular models



Vertical GAA:

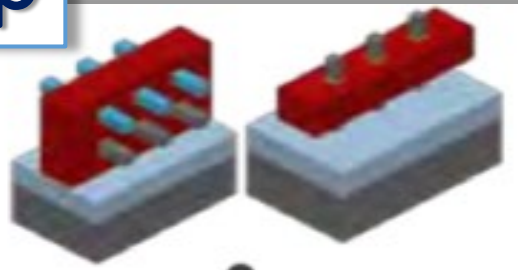






IMEC View of the roadmap

Nanowire/sheet



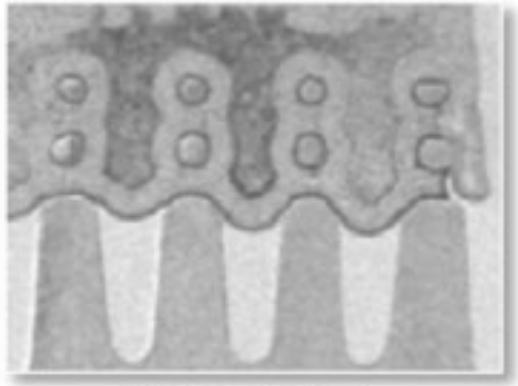
CFET (n-on-p)

VFET

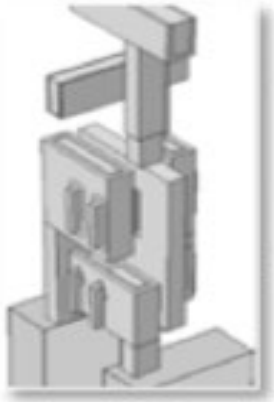
6nm 5nm 4nm 3nm 2nm

2020	2021	2022	2023	2024
48nm 36nm 6.5T	42nm 32nm 6.5T	42nm 32nm 6.5T	36-42nm 21-24nm 5.5T-4.5T	36-42nm 21-24nm 4.5T-3T
				Gate Pitch Metal Pitch # Tracks

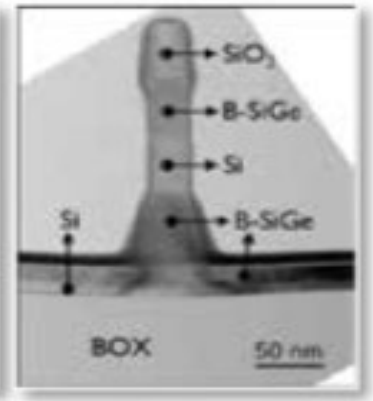
21nm finfet pitch



Nanowire FET

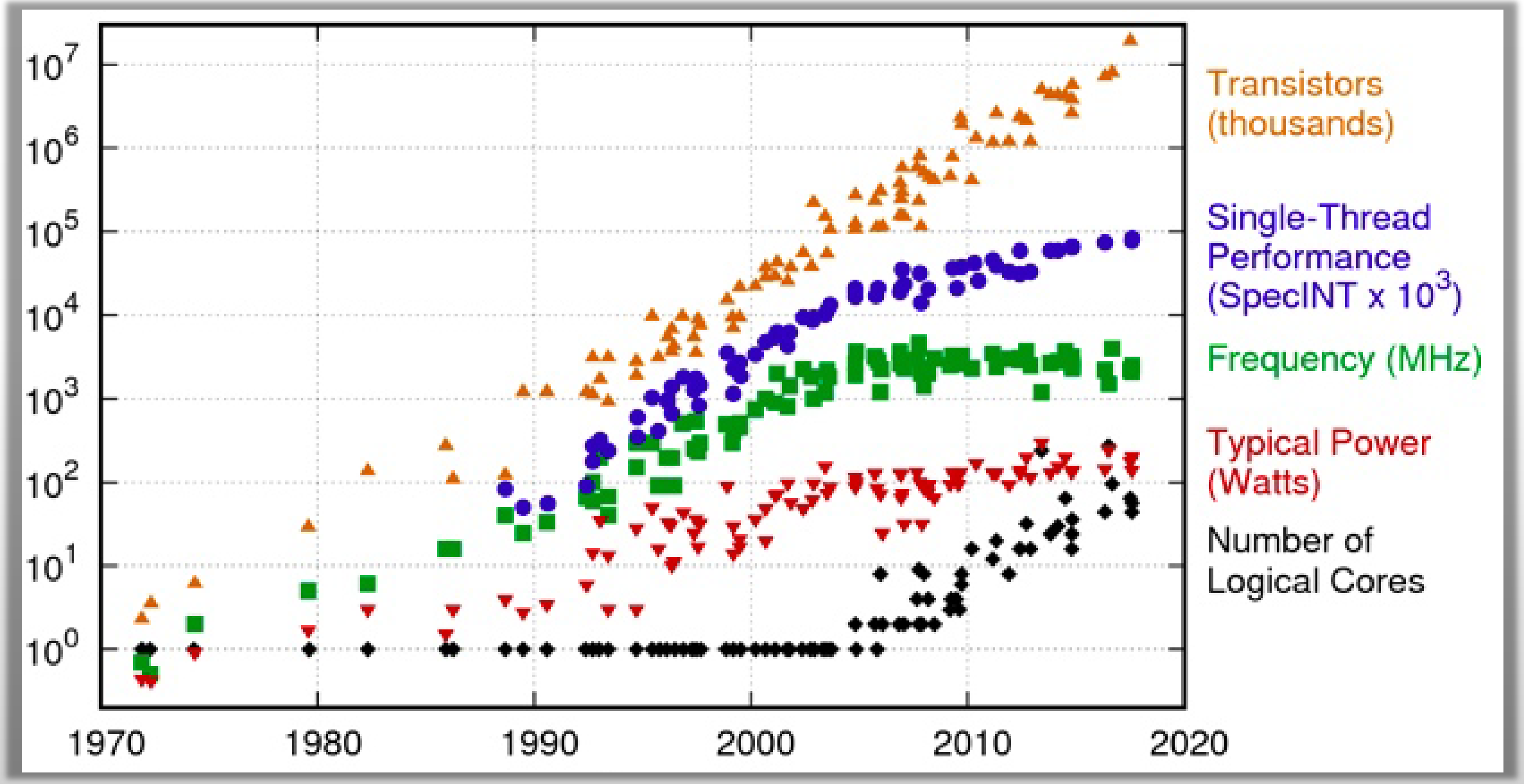


CFET

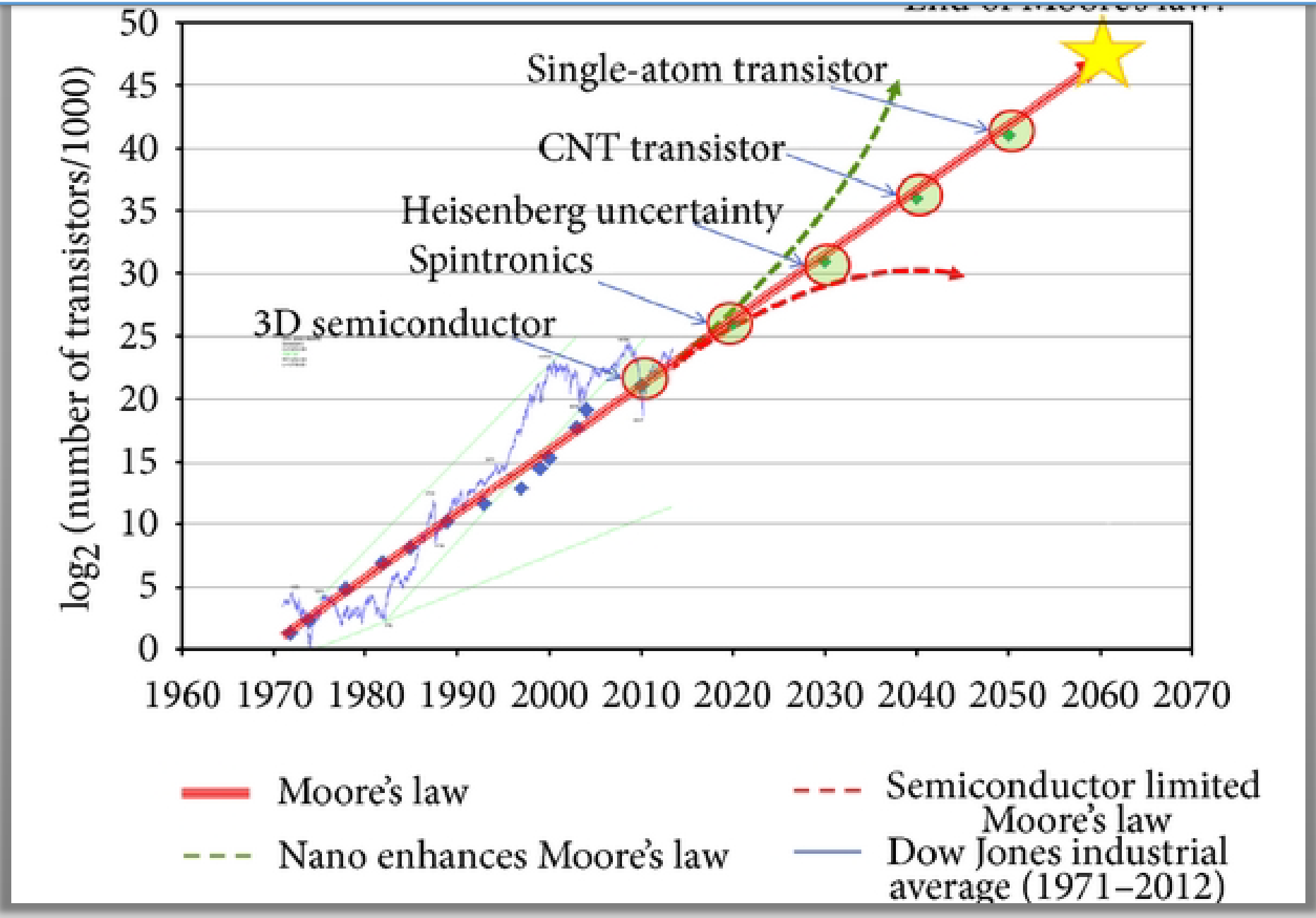


VFET

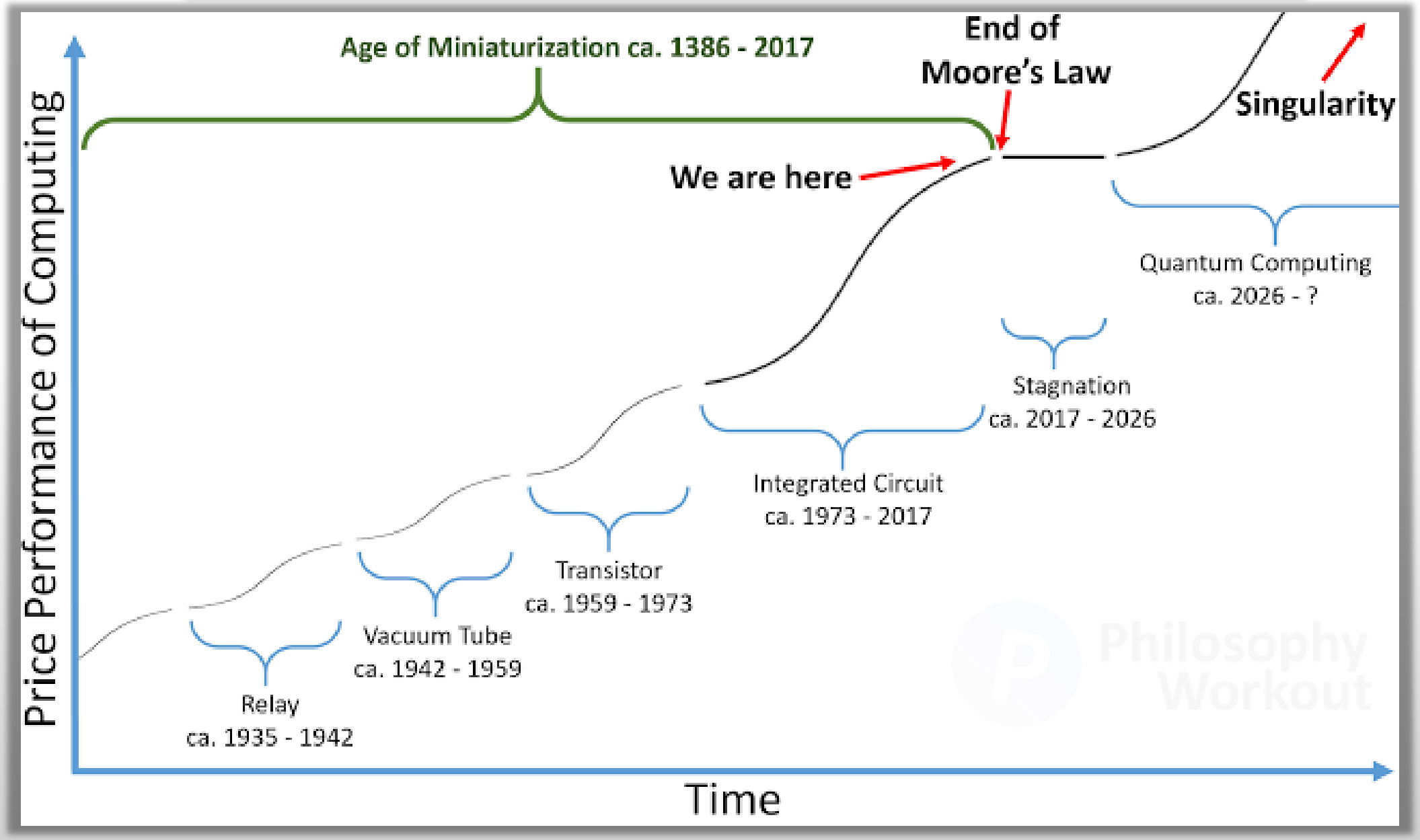
Frequency and performance are not following



Switch to quantum computing: Single atom transistor



Switch to quantum computing: 2026?



NORTHERN ARIZONA UNIVERSITY

Homework #1

Search recent announcements from Intel, AMD, TSMC, and Samsung on their advanced semiconductor node:

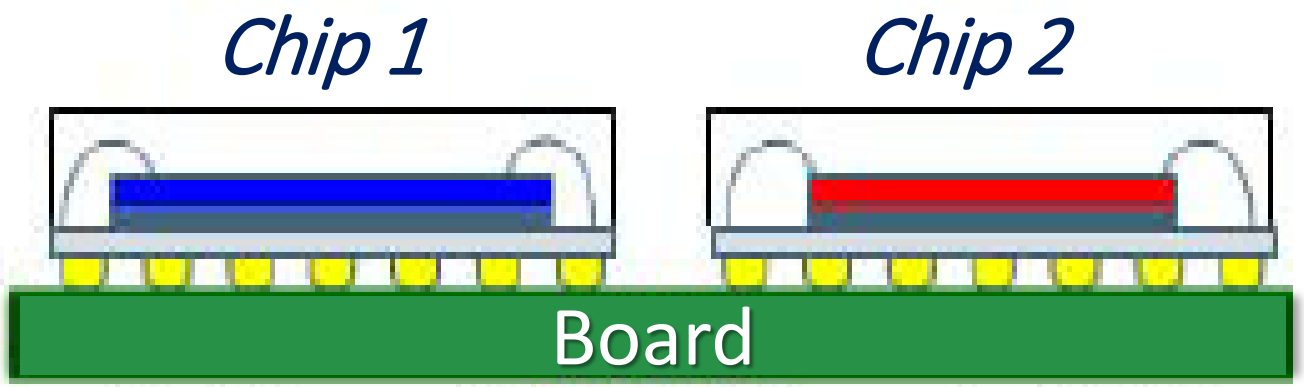
- Who is first?
- Who is behind?
- Explain why.

NORTHERN ARIZONA UNIVERSITY

1 From Micro to Nano-electronics

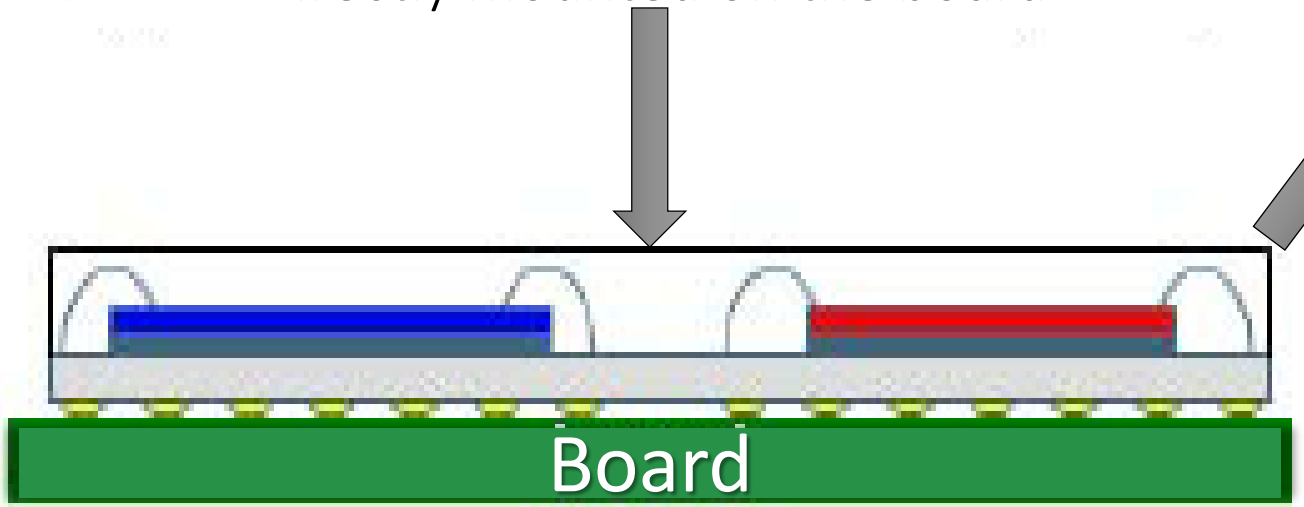
- 1- Motivation for INF633/EE599
- 2- From 1µm to 45nm – the Moore law
  - The MOS transistor - limitations
  - Path to 45nm
- 3- From 45nm to 10nm – 3D transistors
- 4- From 10nm to 1nm – Nanotubes
- 5- 3D integration – Stacking silicon together

From PCB (Printed Circuit Board) to TSV (Through Silicon Via)



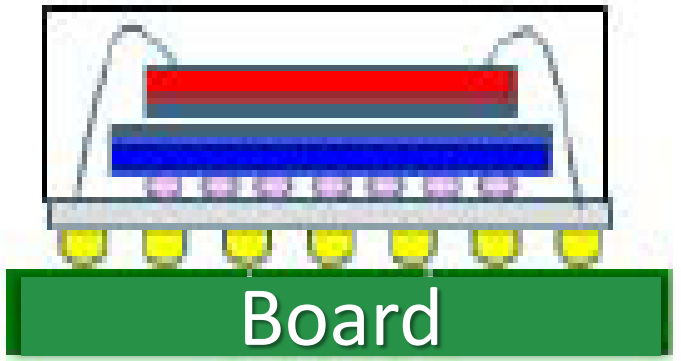
(a) Printed Circuit Board (PCB)

Directly mounted on the board



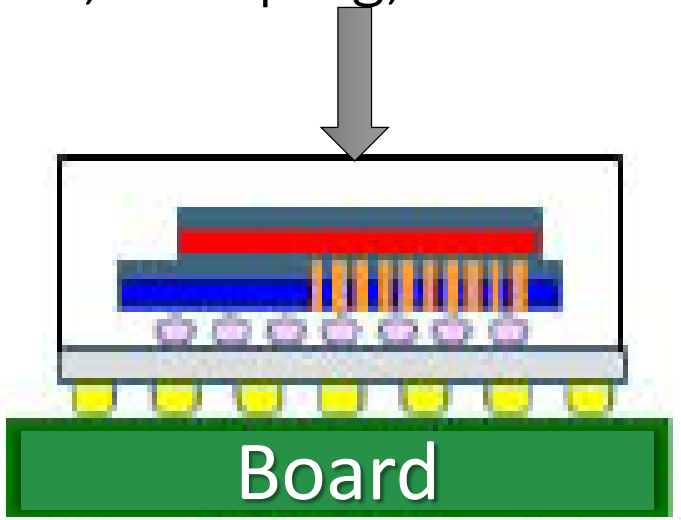
(b) Multi-Chip Package (MCP)

Interposer and wire bonding



(c) System in Package (SIP)

Interposer, Bumping, wire bonding

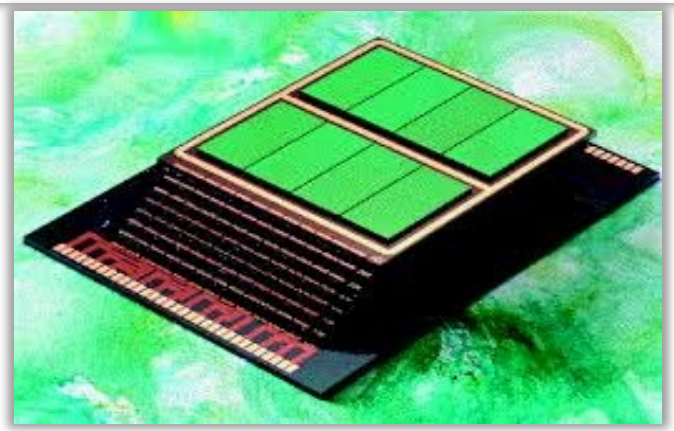


(d) Though Silicon Via (TSV)

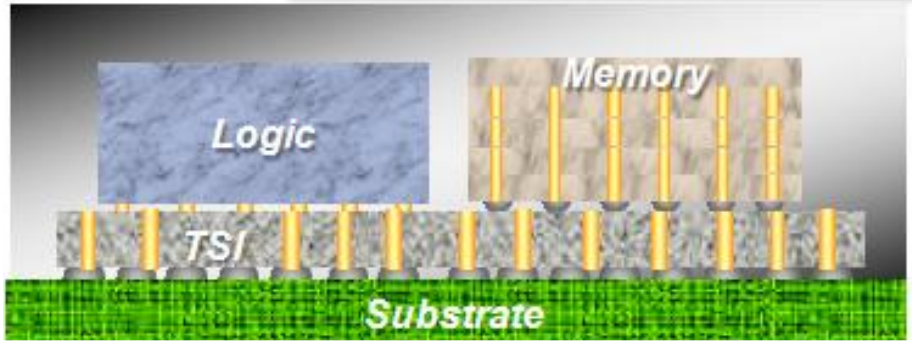
Interposer, Bumping, 3D-TSV

Path to higher performance

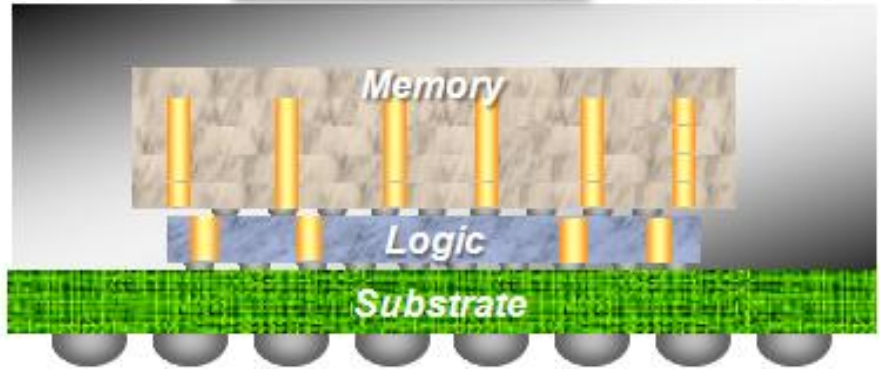
SIP - wire bonding



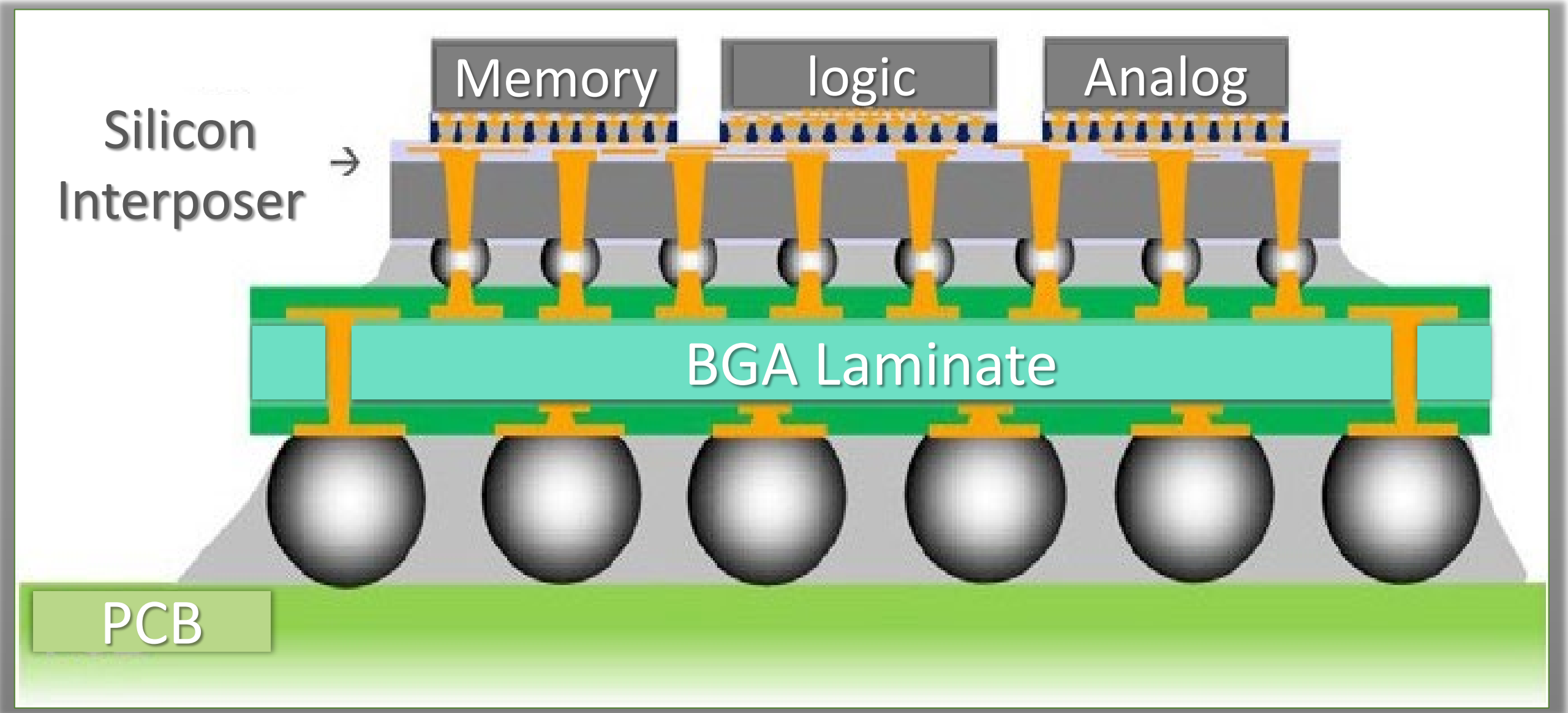
2.5 D TSV - interposer



3 D TSV

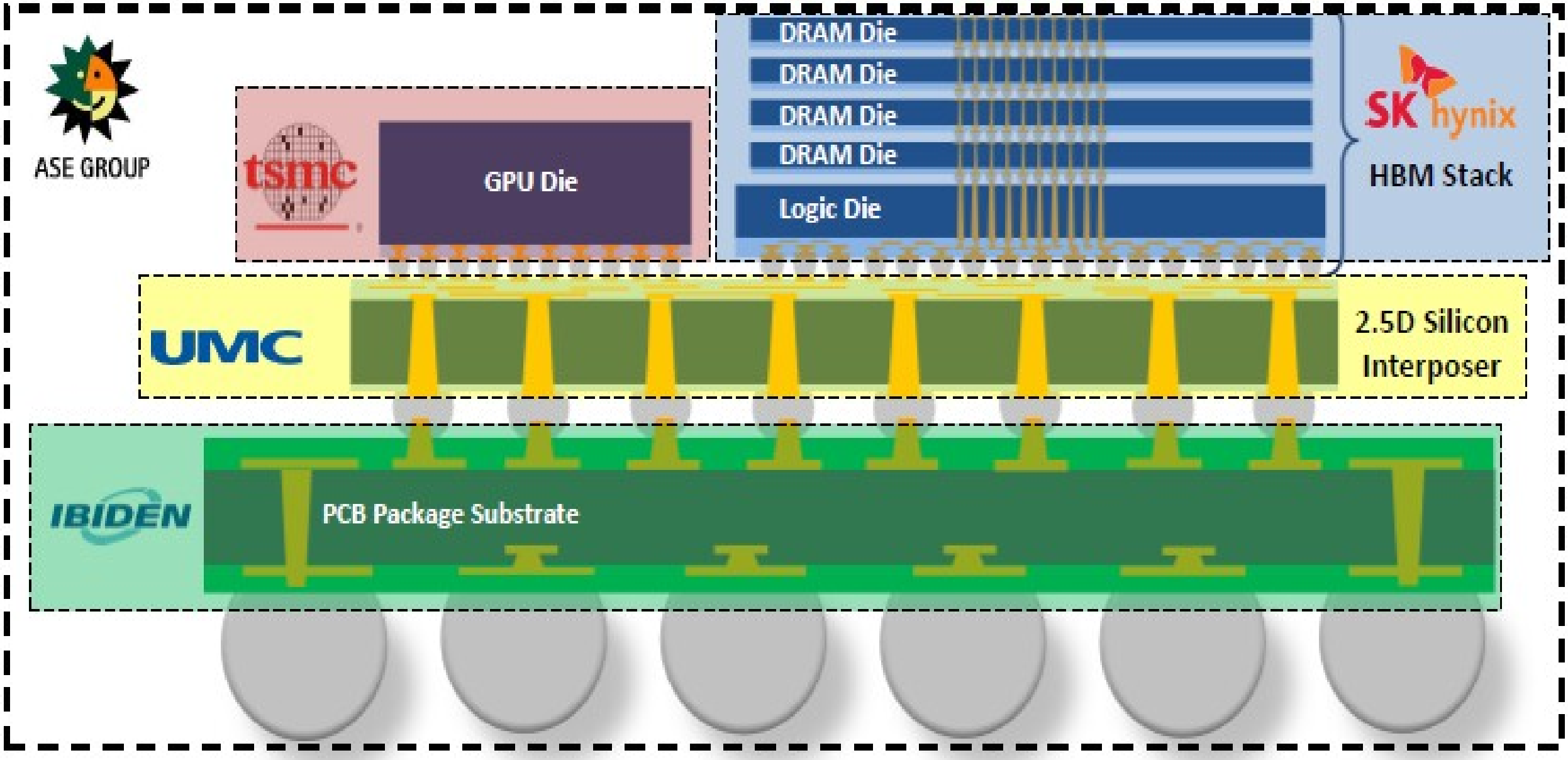


Example of 2.5 D TSV with interposer and Multi-chip

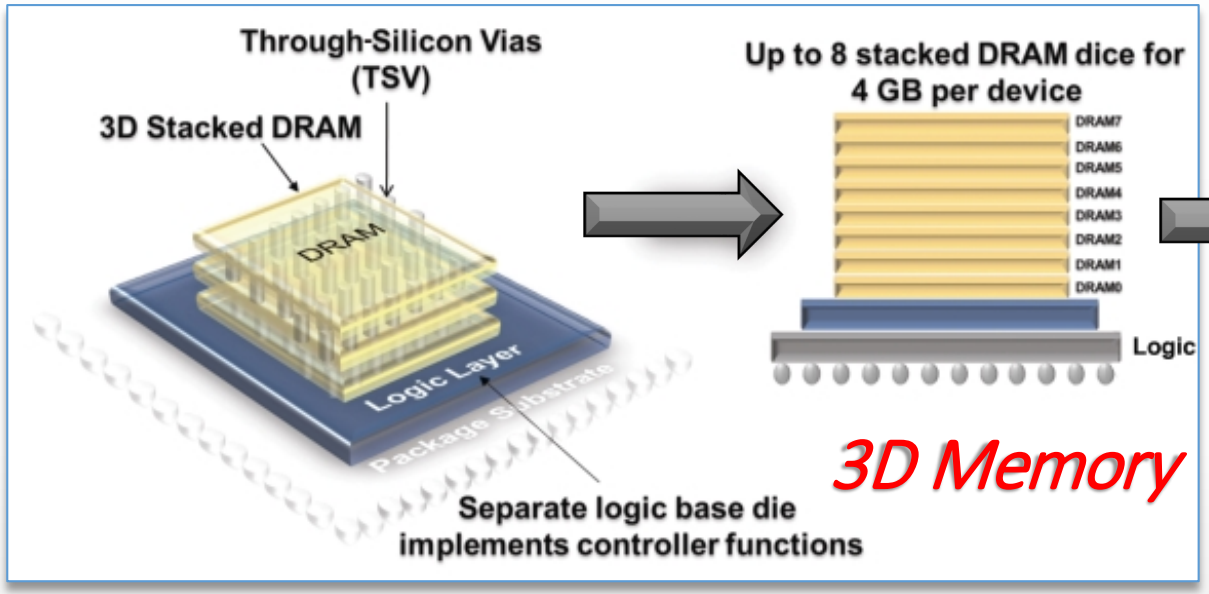


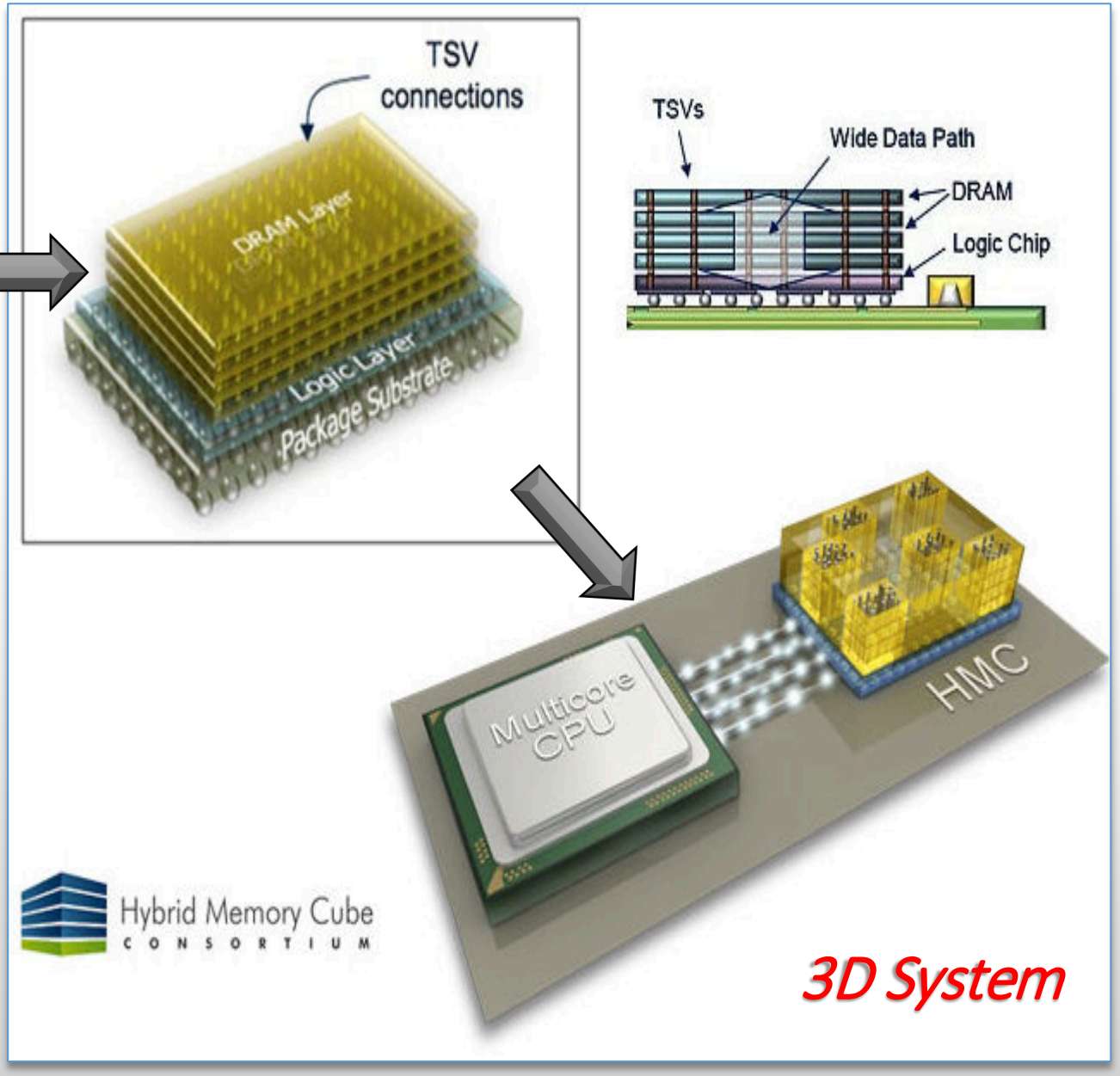
Example of 3 D TSV with 2.5 D system

AMD



DRAM technology: 3D & System integration

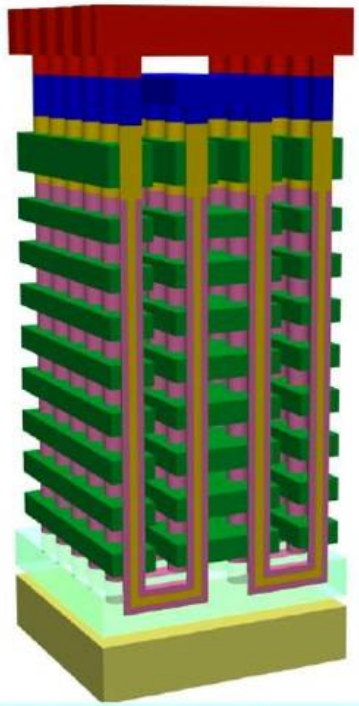


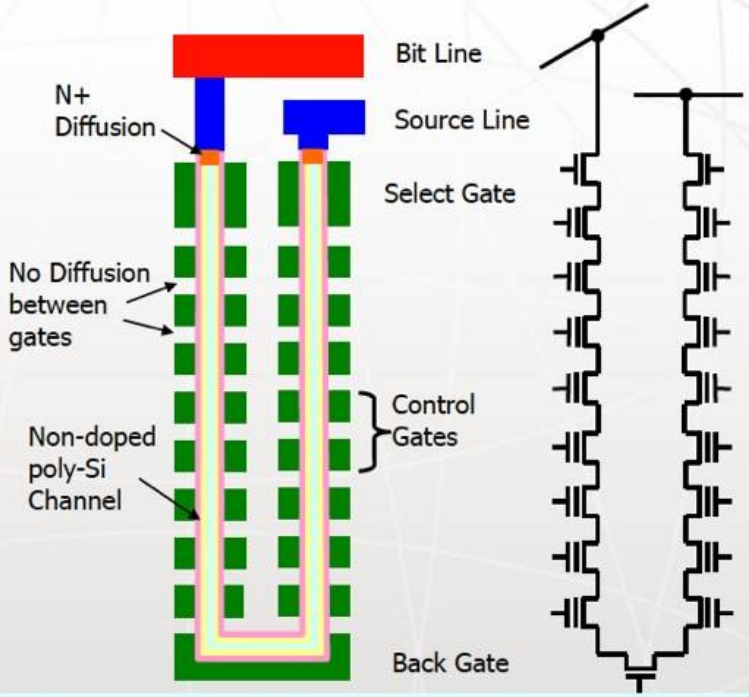


- Up to 16 DRAM chips stacked
- 3D : Memory arrays with logic chip
- 2.5D: Interposer to connect CPU

NAND : 3D integration

P-BiCS Flash



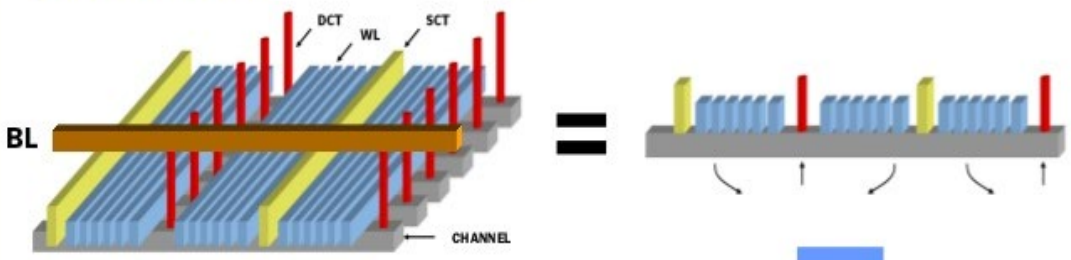


P-BiCS has "U" shaped NAND string with back gate to reduce parasitic resistance of bottom portion. There is no diffusion between CGs. Select gate has asymmetric source and drain structure to reduce off current.

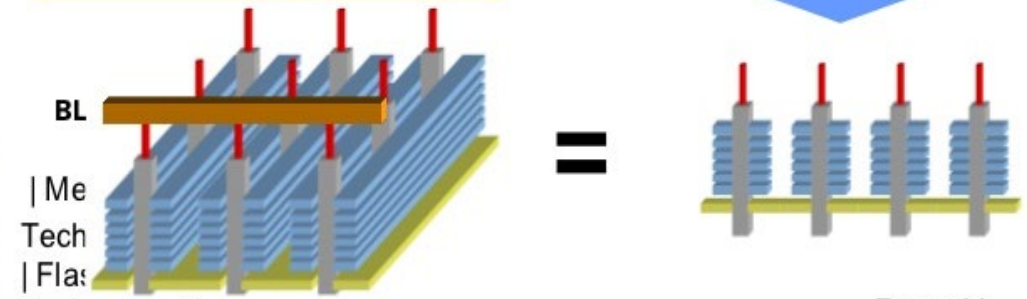
Concept of Vertical String 3D NAND

- 3D is simple rotation of 2D (Schematically the same)

2D NAND Flash



3D Vertical String NAND Flash



Rotation

Thank You!!!

Q & A

bertrand.cambou@nau.edu